



Junos[®] Space

Service Now User Guide

Release

11.1



Published: 2011-03-16

Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, California 94089
USA
408-745-2000
www.juniper.net

This product includes the Envoy SNMP Engine, developed by Epilogue Technology, an Integrated Systems Company. Copyright © 1986-1997, Epilogue Technology Corporation. All rights reserved. This program and its documentation were developed at private expense, and no part of them is in the public domain.

This product includes memory allocation software developed by Mark Moraes, copyright © 1988, 1989, 1993, University of Toronto.

This product includes FreeBSD software developed by the University of California, Berkeley, and its contributors. All of the documentation and software included in the 4.4BSD and 4.4BSD-Lite Releases is copyrighted by the Regents of the University of California. Copyright © 1979, 1980, 1983, 1986, 1988, 1989, 1991, 1992, 1993, 1994. The Regents of the University of California. All rights reserved.

GateD software copyright © 1995, the Regents of the University. All rights reserved. Gate Daemon was originated and developed through release 3.0 by Cornell University and its collaborators. Gated is based on Kirton's EGP, UC Berkeley's routing daemon (routed), and DCN's HELLO routing protocol. Development of Gated has been supported in part by the National Science Foundation. Portions of the GateD software copyright © 1988, Regents of the University of California. All rights reserved. Portions of the GateD software copyright © 1991, D. L. S. Associates.

This product includes software developed by Maker Communications, Inc., copyright © 1996, 1997, Maker Communications, Inc.

Juniper Networks, Junos, Steel-Belted Radius, NetScreen, and ScreenOS are registered trademarks of Juniper Networks, Inc. in the United States and other countries. The Juniper Networks Logo, the Junos logo, and JunosE are trademarks of Juniper Networks, Inc. All other trademarks, service marks, registered trademarks, or registered service marks are the property of their respective owners.

Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

Products made or sold by Juniper Networks or components thereof might be covered by one or more of the following patents that are owned by or licensed to Juniper Networks: U.S. Patent Nos. 5,473,599, 5,905,725, 5,909,440, 6,192,051, 6,333,650, 6,359,479, 6,406,312, 6,429,706, 6,459,579, 6,493,347, 6,538,518, 6,538,899, 6,552,918, 6,567,902, 6,578,186, and 6,590,785.

Junos Space Service Now User Guide
Release 11.1, Revision 1
Copyright © 2011, Juniper Networks, Inc.
All rights reserved.

Revision History
February 2011—R1 Junos Space Service Now User Guide, Release 11.1

The information in this document is current as of the date listed in the revision history.

YEAR 2000 NOTICE

Juniper Networks hardware and software products are Year 2000 compliant. The Junos OS has no known time-related limitations through the year 2038. However, the NTP application is known to have some difficulty in the year 2036.

END USER LICENSE AGREEMENT

READ THIS END USER LICENSE AGREEMENT ("AGREEMENT") BEFORE DOWNLOADING, INSTALLING, OR USING THE SOFTWARE. BY DOWNLOADING, INSTALLING, OR USING THE SOFTWARE OR OTHERWISE EXPRESSING YOUR AGREEMENT TO THE TERMS CONTAINED HEREIN, YOU (AS CUSTOMER OR IF YOU ARE NOT THE CUSTOMER, AS A REPRESENTATIVE/AGENT AUTHORIZED TO BIND THE CUSTOMER) CONSENT TO BE BOUND BY THIS AGREEMENT. IF YOU DO NOT OR CANNOT AGREE TO THE TERMS CONTAINED HEREIN, THEN (A) DO NOT DOWNLOAD, INSTALL, OR USE THE SOFTWARE, AND (B) YOU MAY CONTACT JUNIPER NETWORKS REGARDING LICENSE TERMS.

1. **The Parties.** The parties to this Agreement are (i) Juniper Networks, Inc. (if the Customer's principal office is located in the Americas) or Juniper Networks (Cayman) Limited (if the Customer's principal office is located outside the Americas) (such applicable entity being referred to herein as "Juniper"), and (ii) the person or organization that originally purchased from Juniper or an authorized Juniper reseller the applicable license(s) for use of the Software ("Customer") (collectively, the "Parties").

2. **The Software.** In this Agreement, "Software" means the program modules and features of the Juniper or Juniper-supplied software, for which Customer has paid the applicable license or support fees to Juniper or an authorized Juniper reseller, or which was embedded by Juniper in equipment which Customer purchased from Juniper or an authorized Juniper reseller. "Software" also includes updates, upgrades and new releases of such software. "Embedded Software" means Software which Juniper has embedded in or loaded onto the Juniper equipment and any updates, upgrades, additions or replacements which are subsequently embedded in or loaded onto the equipment.

3. **License Grant.** Subject to payment of the applicable fees and the limitations and restrictions set forth herein, Juniper grants to Customer a non-exclusive and non-transferable license, without right to sublicense, to use the Software, in executable form only, subject to the following use restrictions:

- a. Customer shall use Embedded Software solely as embedded in, and for execution on, Juniper equipment originally purchased by Customer from Juniper or an authorized Juniper reseller.
- b. Customer shall use the Software on a single hardware chassis having a single processing unit, or as many chassis or processing units for which Customer has paid the applicable license fees; provided, however, with respect to the Steel-Belted Radius or Odyssey Access Client software only, Customer shall use such Software on a single computer containing a single physical random access memory space and containing any number of processors. Use of the Steel-Belted Radius or IMS AAA software on multiple computers or virtual machines (e.g., Solaris zones) requires multiple licenses, regardless of whether such computers or virtualizations are physically contained on a single chassis.
- c. Product purchase documents, paper or electronic user documentation, and/or the particular licenses purchased by Customer may specify limits to Customer's use of the Software. Such limits may restrict use to a maximum number of seats, registered endpoints, concurrent users, sessions, calls, connections, subscribers, clusters, nodes, realms, devices, links, ports or transactions, or require the purchase of separate licenses to use particular features, functionalities, services, applications, operations, or capabilities, or provide throughput, performance, configuration, bandwidth, interface, processing, temporal, or geographical limits. In addition, such limits may restrict the use of the Software to managing certain kinds of networks or require the Software to be used only in conjunction with other specific Software. Customer's use of the Software shall be subject to all such limitations and purchase of all applicable licenses.
- d. For any trial copy of the Software, Customer's right to use the Software expires 30 days after download, installation or use of the Software. Customer may operate the Software after the 30-day trial period only if Customer pays for a license to do so. Customer may not extend or create an additional trial period by re-installing the Software after the 30-day trial period.
- e. The Global Enterprise Edition of the Steel-Belted Radius software may be used by Customer only to manage access to Customer's enterprise network. Specifically, service provider customers are expressly prohibited from using the Global Enterprise Edition of the Steel-Belted Radius software to support any commercial network access services.

The foregoing license is not transferable or assignable by Customer. No license is granted herein to any user who did not originally purchase the applicable license(s) for the Software from Juniper or an authorized Juniper reseller.

4. **Use Prohibitions.** Notwithstanding the foregoing, the license provided herein does not permit the Customer to, and Customer agrees not to and shall not: (a) modify, unbundle, reverse engineer, or create derivative works based on the Software; (b) make unauthorized copies of the Software (except as necessary for backup purposes); (c) rent, sell, transfer, or grant any rights in and to any copy of the Software, in any form, to any third party; (d) remove any proprietary notices, labels, or marks on or in any copy of the Software or any product in which the Software is embedded; (e) distribute any copy of the Software to any third party, including as may be embedded in Juniper equipment sold in the secondhand market; (f) use any 'locked' or key-restricted feature, function, service, application, operation, or capability without first purchasing the applicable license(s) and obtaining a valid key from Juniper, even if such feature, function, service, application, operation, or capability is enabled without a key; (g) distribute any key for the Software provided by Juniper to any third party; (h) use the

Software in any manner that extends or is broader than the uses purchased by Customer from Juniper or an authorized Juniper reseller; (i) use Embedded Software on non-Juniper equipment; (j) use Embedded Software (or make it available for use) on Juniper equipment that the Customer did not originally purchase from Juniper or an authorized Juniper reseller; (k) disclose the results of testing or benchmarking of the Software to any third party without the prior written consent of Juniper; or (l) use the Software in any manner other than as expressly provided herein.

5. **Audit.** Customer shall maintain accurate records as necessary to verify compliance with this Agreement. Upon request by Juniper, Customer shall furnish such records to Juniper and certify its compliance with this Agreement.

6. **Confidentiality.** The Parties agree that aspects of the Software and associated documentation are the confidential property of Juniper. As such, Customer shall exercise all reasonable commercial efforts to maintain the Software and associated documentation in confidence, which at a minimum includes restricting access to the Software to Customer employees and contractors having a need to use the Software for Customer's internal business purposes.

7. **Ownership.** Juniper and Juniper's licensors, respectively, retain ownership of all right, title, and interest (including copyright) in and to the Software, associated documentation, and all copies of the Software. Nothing in this Agreement constitutes a transfer or conveyance of any right, title, or interest in the Software or associated documentation, or a sale of the Software, associated documentation, or copies of the Software.

8. **Warranty, Limitation of Liability, Disclaimer of Warranty.** The warranty applicable to the Software shall be as set forth in the warranty statement that accompanies the Software (the "Warranty Statement"). Nothing in this Agreement shall give rise to any obligation to support the Software. Support services may be purchased separately. Any such support shall be governed by a separate, written support services agreement. TO THE MAXIMUM EXTENT PERMITTED BY LAW, JUNIPER SHALL NOT BE LIABLE FOR ANY LOST PROFITS, LOSS OF DATA, OR COSTS OR PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES, OR FOR ANY SPECIAL, INDIRECT, OR CONSEQUENTIAL DAMAGES ARISING OUT OF THIS AGREEMENT, THE SOFTWARE, OR ANY JUNIPER OR JUNIPER-SUPPLIED SOFTWARE. IN NO EVENT SHALL JUNIPER BE LIABLE FOR DAMAGES ARISING FROM UNAUTHORIZED OR IMPROPER USE OF ANY JUNIPER OR JUNIPER-SUPPLIED SOFTWARE. EXCEPT AS EXPRESSLY PROVIDED IN THE WARRANTY STATEMENT TO THE EXTENT PERMITTED BY LAW, JUNIPER DISCLAIMS ANY AND ALL WARRANTIES IN AND TO THE SOFTWARE (WHETHER EXPRESS, IMPLIED, STATUTORY, OR OTHERWISE), INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT. IN NO EVENT DOES JUNIPER WARRANT THAT THE SOFTWARE, OR ANY EQUIPMENT OR NETWORK RUNNING THE SOFTWARE, WILL OPERATE WITHOUT ERROR OR INTERRUPTION, OR WILL BE FREE OF VULNERABILITY TO INTRUSION OR ATTACK. In no event shall Juniper's or its suppliers' or licensors' liability to Customer, whether in contract, tort (including negligence), breach of warranty, or otherwise, exceed the price paid by Customer for the Software that gave rise to the claim, or if the Software is embedded in another Juniper product, the price paid by Customer for such other product. Customer acknowledges and agrees that Juniper has set its prices and entered into this Agreement in reliance upon the disclaimers of warranty and the limitations of liability set forth herein, that the same reflect an allocation of risk between the Parties (including the risk that a contract remedy may fail of its essential purpose and cause consequential loss), and that the same form an essential basis of the bargain between the Parties.

9. **Termination.** Any breach of this Agreement or failure by Customer to pay any applicable fees due shall result in automatic termination of the license granted herein. Upon such termination, Customer shall destroy or return to Juniper all copies of the Software and related documentation in Customer's possession or control.

10. **Taxes.** All license fees payable under this agreement are exclusive of tax. Customer shall be responsible for paying Taxes arising from the purchase of the license, or importation or use of the Software. If applicable, valid exemption documentation for each taxing jurisdiction shall be provided to Juniper prior to invoicing, and Customer shall promptly notify Juniper if their exemption is revoked or modified. All payments made by Customer shall be net of any applicable withholding tax. Customer will provide reasonable assistance to Juniper in connection with such withholding taxes by promptly: providing Juniper with valid tax receipts and other required documentation showing Customer's payment of any withholding taxes; completing appropriate applications that would reduce the amount of withholding tax to be paid; and notifying and assisting Juniper in any audit or tax proceeding related to transactions hereunder. Customer shall comply with all applicable tax laws and regulations, and Customer will promptly pay or reimburse Juniper for all costs and damages related to any liability incurred by Juniper as a result of Customer's non-compliance or delay with its responsibilities herein. Customer's obligations under this Section shall survive termination or expiration of this Agreement.

11. **Export.** Customer agrees to comply with all applicable export laws and restrictions and regulations of any United States and any applicable foreign agency or authority, and not to export or re-export the Software or any direct product thereof in violation of any such restrictions, laws or regulations, or without all necessary approvals. Customer shall be liable for any such violations. The version of the Software supplied to Customer may contain encryption or other capabilities restricting Customer's ability to export the Software without an export license.

12. **Commercial Computer Software.** The Software is "commercial computer software" and is provided with restricted rights. Use, duplication, or disclosure by the United States government is subject to restrictions set forth in this Agreement and as provided in DFARS 227.7201 through 227.7202-4, FAR 12.212, FAR 27.405(b)(2), FAR 52.227-19, or FAR 52.227-14 (ALT III) as applicable.

13. **Interface Information.** To the extent required by applicable law, and at Customer's written request, Juniper shall provide Customer with the interface information needed to achieve interoperability between the Software and another independently created program, on payment of applicable fee, if any. Customer shall observe strict obligations of confidentiality with respect to such information and shall use such information in compliance with any applicable terms and conditions upon which Juniper makes such information available.

14. **Third Party Software.** Any licensor of Juniper whose software is embedded in the Software and any supplier of Juniper whose products or technology are embedded in (or services are accessed by) the Software shall be a third party beneficiary with respect to this Agreement, and such licensor or vendor shall have the right to enforce this Agreement in its own name as if it were Juniper. In addition, certain third party software may be provided with the Software and is subject to the accompanying license(s), if any, of its respective owner(s). To the extent portions of the Software are distributed under and subject to open source licenses obligating Juniper to make the source code for such portions publicly available (such as the GNU General Public License ("GPL") or the GNU Library General Public License ("LGPL")), Juniper will make such source code portions (including Juniper modifications, as appropriate) available upon request for a period of up to three years from the date of distribution. Such request can be made in writing to Juniper Networks, Inc., 1194 N. Mathilda Ave., Sunnyvale, CA 94089, ATTN: General Counsel. You may obtain a copy of the GPL at <http://www.gnu.org/licenses/gpl.html>, and a copy of the LGPL at <http://www.gnu.org/licenses/lgpl.html>.

15. **Miscellaneous.** This Agreement shall be governed by the laws of the State of California without reference to its conflicts of laws principles. The provisions of the U.N. Convention for the International Sale of Goods shall not apply to this Agreement. For any disputes arising under this Agreement, the Parties hereby consent to the personal and exclusive jurisdiction of, and venue in, the state and federal courts within Santa Clara County, California. This Agreement constitutes the entire and sole agreement between Juniper and the Customer with respect to the Software, and supersedes all prior and contemporaneous agreements relating to the Software, whether oral or written (including any inconsistent terms contained in a purchase order), except that the terms of a separate written agreement executed by an authorized Juniper representative and Customer shall govern to the extent such terms are inconsistent or conflict with terms contained herein. No modification to this Agreement nor any waiver of any rights hereunder shall be effective unless expressly assented to in writing by the party to be charged. If any portion of this Agreement is held invalid, the Parties agree that such invalidity shall not affect the validity of the remainder of this Agreement. This Agreement and associated documentation has been written in the English language, and the Parties agree that the English version will govern. (For Canada: Les parties aux présentes confirment leur volonté que cette convention de même que tous les documents y compris tout avis qui s'y rattache, soient rédigés en langue anglaise. (Translation: The parties confirm that this Agreement and all related documentation is and will be in the English language)).

Table of Contents

	About the Documentation	xv
	Junos Space Documentation and Release Notes	xv
	Documentation Conventions	xv
	Documentation Feedback	xvi
	Requesting Technical Support	xvi
	Self-Help Online Tools and Resources	xvii
	Opening a Case with JTAC	xvii
Part 1	Service Now Overview	
Chapter 1	Service Now Overview	3
	Service Now Overview	3
Chapter 2	Upgrading Service Now	7
	Upgrading Service Now	7
Chapter 3	Service Now Modes	9
	Service Now Modes	9
	Overview	9
	Activating End Customer and Partner Proxy Modes	11
Chapter 4	Service Now Dashboard and Workspaces Overview	13
	Service Now Dashboard Overview	13
	Service Now Workspaces	13
	Dashboard Gadgets	14
	Platforms with Most Incidents	14
	Devices with Most Incidents	14
	Service Now Notices (Upgrade and Contract Notice)	15
Chapter 5	Service Now Icons	17
	Service Now Icons	17
Chapter 6	User Roles	23
	Service Now User Roles	23
Part 2	Using the Service Now Getting Started Assistant	
Chapter 7	Service Now Getting Started Assistant Usage Overview	27
	Service Now Getting Started Assistant Usage Overview	27
Part 3	Service Central	
	Service Central Overview	29

Chapter 8	Incidents	31
	Incidents Overview	31
	Assigning an Incident Owner	32
	Flagging an Incident to a User	33
	Checking Incident Status Updates	34
	Exporting Incident Data	34
	Deleting an Incident	35
	Submitting an Incident to Juniper Support Systems	36
	Viewing Incident Details	36
	Viewing a Case in the Case Manager	37
	Modifying Submit Case Options	38
	Updating an End Customer Case	39
Chapter 9	Information	41
	Messages Overview	41
	Assigning Ownership	42
	Flagging a Message to Users	42
	Deleting a Message	43
	Scanning a Message for Impact	43
	Assigning a Message to a Connected Member	43
	Device Snapshots Overview	45
	Exporting Device Data into HTML	45
	Deleting Device Snapshots	46
	Viewing Device Snapshot Details	46
Chapter 10	JMB Errors	49
	JMB Errors	49
	Downloading JMB Errors	49
	Deleting JMB Errors	50
Chapter 11	Notifications	51
	Notification Policies Overview	51
	Creating and Editing a Notification Policy	52
	Enabling or Disabling a Notification Policy	57
	Deleting a Notification Policy	57
Part 4	Administration	
	Administration Overview	59
Chapter 12	Organizations	63
	Organizations Overview	63
	Adding an Organization	65
	Adding a Connected Member	67
	Modifying Organization Parameters	68
	Deleting an Organization	69
	Test the Connection to JSS	70
	Viewing Messages Assigned to a Connected Member	70
	Running an Organization in Test Mode	71

Chapter 13	Device Groups	73
	Device Groups Overview	73
	Creating a Device Group	73
	Modifying Device Groups	74
	Deleting Device Groups	75
Chapter 14	Devices	77
	Service Now Devices Overview	77
	Adding Devices from the Platform	80
	Installing an Event Profile on Devices Using Service Now	80
	Installing AI-Scripts Manually on Devices	82
	Uninstalling Event Profiles from Devices	84
	Exporting Device Data in CSV and Excel Format	84
	Deleting a Device	85
	Associating Devices to a Device Group	85
Chapter 15	Event Profiles and Script Bundles	87
	Event Profiles Overview	87
	Adding an Event Profile	89
	Cloning an Event Profile	91
	Deleting Event Profiles	92
	Viewing an Event Profile	93
	Pushing an Event Profile to Devices	94
	Displaying Devices Associated with an Event Profile	95
	Setting an Event Profile as Default	96
	Exporting Events Data in Excel Format	97
	Script Bundles Overview	98
	What AI-Scripts Do	98
	Events Detected by AI-Scripts	98
	JMB Contents	98
	Managing Script Bundles using Service Now	99
	Adding a Script Bundle to Service Now	99
	Setting a Script Bundle as Default	100
	Deleting a Script Bundle from Service Now	101
Chapter 16	Global Settings	103
	Configuring Global Settings	103
	Adding an SNMP Server	106
	Editing and Deleting an SNMP Server	107
	Configuring Proxy Server Settings	108
Part 5	Index	
	Index	113

List of Figures

Part 1	Service Now Overview	
Chapter 4	Service Now Dashboard and Workspaces Overview	13
	Figure 1: Platform with Most Incidents Gadget	14
	Figure 2: Devices with Most Incidents Gadget	15
Part 3	Service Central	
Chapter 8	Incidents	31
	Figure 3: Export JMB to HTML Dialog Box	35
	Figure 4: End Customer Cases Dialog Box	40
Chapter 9	Information	41
	Figure 5: Choose Connected Members Dialog Box	44
	Figure 6: View JMB Dialog Box	47
Chapter 11	Notifications	51
	Figure 7: Create Notifications dialog box	53
Part 4	Administration	
Chapter 12	Organizations	63
	Figure 8: Manage Organizations Page	64
	Figure 9: Add Member Dialog Box	67
	Figure 10: Modify Organization Dialog Box	69
	Figure 11: Messages Assigned to Connected Member page	71
Chapter 14	Devices	77
	Figure 12: Service Now Devices Page	78
	Figure 13: Install Event Profile Dialog Box	81
Chapter 15	Event Profiles and Script Bundles	87
	Figure 14: View Event Profiles Page	88
	Figure 15: Clone Event Profile page	91
	Figure 16: Event difference display dialog box	92
	Figure 17: Install Event Profile Dialog Box	94
	Figure 18: Manage Service Now Devices page Displaying Device Associated to an Event Profile	96
	Figure 19: View Event Profiles page	97
	Figure 20: Administration: Add Script Bundle Dialog Box	100

List of Tables

	About the Documentation	xv
	Table 1: Notice Icons	xvi
Part 1	Service Now Overview	
Chapter 3	Service Now Modes	9
	Table 2: Tasks Enabled for Service Now Modes	10
Chapter 4	Service Now Dashboard and Workspaces Overview	13
	Table 3: Service Now Workspaces	13
Chapter 5	Service Now Icons	17
	Table 4: Inventory Page Icon Description	17
	Table 5: Task Icons	20
Chapter 6	User Roles	23
	Table 6: Predefined Service Now User Roles and Permissions	24
Part 3	Service Central	
Chapter 11	Notifications	51
	Table 7: Notification Policies Table Column Descriptions	51
	Table 8: Create Notification Policy Page Field Descriptions	54
	Table 9: Notification Policy Table Command Button Descriptions	56
Part 4	Administration	
Chapter 12	Organizations	63
	Table 10: Organization Column Descriptions	64
	Table 11: Organization Credentials Page Field Descriptions	66
Chapter 14	Devices	77
	Table 12: Service Now Devices Column Descriptions	78
Chapter 15	Event Profiles and Script Bundles	87
	Table 13: Add Event Profile Page Field Descriptions	90
Chapter 16	Global Settings	103
	Table 14: Global Settings Command Buttons	104
	Table 15: Global Settings Parameters	105

About the Documentation

- Junos Space Documentation and Release Notes on page xv
- Documentation Conventions on page xv
- Documentation Feedback on page xvi
- Requesting Technical Support on page xvi

Junos Space Documentation and Release Notes

For a list of related Junos Space documentation, see <http://www.juniper.net/techpubs/>.

If the information in the latest release notes differs from the information in the documentation, follow the *Junos Space Release Notes*.

To obtain the most current version of all Juniper Networks[®] technical documentation, see the product documentation page on the Juniper Networks website at <http://www.juniper.net/techpubs/>.

Juniper Networks supports a technical book program to publish books by Juniper Networks engineers and subject matter experts with book publishers around the world. These books go beyond the technical documentation to explore the nuances of network architecture, deployment, and administration using the Junos operating system (Junos OS) and Juniper Networks devices. In addition, the Juniper Networks Technical Library, published in conjunction with O'Reilly Media, explores improving network security, reliability, and availability using Junos OS configuration techniques. All the books are for sale at technical bookstores and book outlets around the world. The current list can be viewed at <http://www.juniper.net/books>.

Documentation Conventions

Table 1 on page xvi defines the notice icons used in this guide.

Table 1: Notice Icons

Icon	Meaning	Description
	Informational note	Indicates important features or instructions.
	Caution	Indicates a situation that might result in loss of data or hardware damage.
	Warning	Alerts you to the risk of personal injury or death.
	Laser warning	Alerts you to the risk of personal injury from a laser.

Documentation Feedback

We encourage you to provide feedback, comments, and suggestions so that we can improve the documentation. You can send your comments to techpubs-comments@juniper.net, or fill out the documentation feedback form at <https://www.juniper.net/cgi-bin/docbugreport/>. If you are using e-mail, be sure to include the following information with your comments:

- Document or topic name
- URL or page number
- Software release version (if applicable)

Requesting Technical Support

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active J-Care or JNASC support contract, or are covered under warranty, and need post-sales technical support, you can access our tools and resources online or open a case with JTAC.

- JTAC policies—For a complete understanding of our JTAC procedures and policies, review the *JTAC User Guide* located at <http://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf>.
- Product warranties—For product warranty information, visit <http://www.juniper.net/support/warranty/>.
- JTAC hours of operation—The JTAC centers have resources available 24 hours a day, 7 days a week, 365 days a year.

Self-Help Online Tools and Resources

For quick and easy problem resolution, Juniper Networks has designed an online self-service portal called the Customer Support Center (CSC) that provides you with the following features:

- Find CSC offerings: <http://www.juniper.net/customers/support/>
- Search for known bugs: <http://www2.juniper.net/kb/>
- Find product documentation: <http://www.juniper.net/techpubs/>
- Find solutions and answer questions using our Knowledge Base: <http://kb.juniper.net/>
- Download the latest versions of software and review release notes: <http://www.juniper.net/customers/csc/software/>
- Search technical bulletins for relevant hardware and software notifications: <https://www.juniper.net/alerts/>
- Join and participate in the Juniper Networks Community Forum: <http://www.juniper.net/company/communities/>
- Open a case online in the CSC Case Management tool: <http://www.juniper.net/cm/>

To verify service entitlement by product serial number, use our Serial Number Entitlement (SNE) Tool: <https://tools.juniper.net/SerialNumberEntitlementSearch/>

Opening a Case with JTAC

You can open a case with JTAC on the Web or by telephone.

- Use the Case Management tool in the CSC at <http://www.juniper.net/cm/> .
- Call 1-888-314-JTAC (1-888-314-5822 toll-free in the USA, Canada, and Mexico).

For international or direct-dial options in countries without toll-free numbers, see <http://www.juniper.net/support/requesting-support.html> .

PART 1

Service Now Overview

- Service Now Overview on page 3
- Upgrading Service Now on page 7
- Service Now Modes on page 9
- Service Now Dashboard and Workspaces Overview on page 13
- Service Now Icons on page 17
- User Roles on page 23

CHAPTER 1

Service Now Overview

- Service Now Overview on page 3

Service Now Overview

Service Now is an application that helps automate fault management and accelerate issue resolution. It significantly reduces intervening time by automating support processes and uses device diagnostics for fault monitoring and case automation. The process of obtaining technical support from Juniper Networks is simplified and the time taken to get resolutions is reduced by eliminating time-consuming manual procedures. Your contract with Juniper Networks determines whether Service Now operates in standard mode, end customer mode, or partner proxy mode. These modes in turn determine which tasks are enabled and disabled in Service Now. See “Service Now Modes” on page 9.

To help ensure maximum network uptime, AI-Scripts are installed on devices, which then automatically detect and report incidents to Service Now. When an event, such as a process crash, an application-specific integrated circuit (ASIC) error, or a fan failure, is detected in devices with AI-Scripts enabled, the AI-Scripts create files called Juniper Message Bundles (JMBs). JMBs contain comprehensive information about the device identity, the problem event, and diagnostics. This information is securely transferred to the Junos Space platform. Service Now then notifies users of the new incident by sending an e-mail or an SNMP trap. In addition to reporting incidents, AI-Scripts also send device information regularly in the form of Information Juniper Message Bundles (iJMBs). In Service Now, JMB errors are JMBs that do not comply with the standard data structure that is expected by Service Now or contain unexpected data elements. Service Now identifies these JMBs and displays them on the **Manage JMB Errors** page where they can be viewed and downloaded.

After reviewing information provided in the JMB, you can submit the incidents to Juniper Support Systems (JSS) to create a Juniper Networks Technical Assistance Center (JTAC) case. The cases are processed and analyzed to provide preventive analysis and alerts. Using Service Now, you can track the status of the case. To restrict the amount of information you share with Juniper Networks, you can filter configuration content from iJMBs before submission.

Apart from submitting JMBs to obtain resolutions, you can use Service Now to perform tasks such as assigning an owner (user), flagging users to keep them notified of changes that are made, updating incident status, and deleting JMBs from the Service Now database. The data in incidents and information messages can also be exported into

different file formats such as HTML, CSV, and Excel, and saved on the local file system. In order to receive notifications from Service Now, you can set up notification policies that notify users that need to be kept informed of changes that affect them.

To add multiple devices and organizations you need to obtain a technical support contract with the right level of service. After you have a valid contract, you can submit incidents and iJMBs to JSS for support. Without a valid contract, Service Now runs in demo mode and supports one organization and five devices for 60 days. In this mode, you cannot open technical support cases with JTAC so the connection to JSS fails.

To open technical support cases and share iJMBs with Juniper Networks, you must first set up an organization in Service Now. An organization represents a unique Clarify site ID in JSS that is used to identify customers while providing technical support. After creating an organization, you can test its connectivity with JSS and even set the submission of incidents as test cases. If you are a Juniper Networks partner or a direct customer with multiple distinct networks, you can use multiple Service Now organizations to keep customers or networks separate.

You can group network elements and manage multiple devices as a single entity using Service Now device groups. By associating an organization with one or more device groups, you can maintain groups of devices with similar attributes or uses. Device groups help you control which users have access to which Service Now devices. After you add devices and create device groups, you can perform various operations on them, such as installing or uninstalling AI-Scripts individually on every device or on all the devices in a device group simultaneously. You can even edit their parameters and delete them from the Service Now database.

In addition to monitoring and managing devices, organizations, and device groups, you can incorporate the use of SNMP and proxy servers. SNMP servers act as destinations where traps are sent when a notification policy is triggered. Configuring Service Now to work with a proxy server facilitates all communication to and from JSS to happen through the proxy server ensuring secure transactions.

The Service Now dashboard displays the gadgets and the workspaces that the user can use to perform various tasks. For more information about the Service Now dashboard and icons, see “Service Now Dashboard Overview” on page 13.

To install, upgrade, and uninstall Service Now, you need Junos Space administrator privileges. For more information, see the Adding a Junos Space Application and Uninstalling a Junos Space Application sections in the *Network Application Platform User Guide* at

http://www.juniper.net/techpubs/en_US/junos-space2.0/information-products/topic-collections/junos-space-network-application-platform-pwp/junos-space-network-application-platform-pwp.pdf. You can install, uninstall, or upgrade Service Now even while Junos Space and Junos Space applications are still running.

With different Service Now user privileges, you can perform one or more of the following tasks:

- Add devices to Service Now from the Junos Space platform.
- Add or delete a script bundle.

- Install or uninstall AI-Scripts on devices.
- Add, modify, or delete devices and device groups.
- Associate devices with device groups.
- Add, modify, or delete an organization.
- Submit incidents as test cases.
- Test organization connectivity to JSS.
- Export device data in CSV and Excel formats.
- Configure the global settings (SNMP server and proxy server settings).
- Assign an owner, flag to users, update status of incidents, and delete incidents.
- View and delete iJMBs, and export device data into HTML format.
- Assign an owner, flag to users, and delete an information message.
- View, download, and delete JMBs with errors.
- Create, edit, and delete a notification policy.

**Related
Documentation**

- Service Central Overview on page 29
- Administration Overview on page 59

CHAPTER 2

Upgrading Service Now

- Upgrading Service Now on page 7

Upgrading Service Now

Service Now can be upgraded to up to two versions higher than its current version. For example, Service Now 1.2 can only be upgraded to Service Now versions 1.3 or 1.4. To upgrade from Service Now version 1.2 to a version higher than 1.4, you must first upgrade to version 1.4 and then upgrade again to the required version.

To upgrade Service Now, see Upgrading a Junos Space Application.

When you upgrade Service Now operating in end-customer or partner proxy mode, ensure that the Service Now partner proxy is of the same version as its end-customer Service Now applications or up to 2 versions higher than the versions of the end-customer Service Now applications that it connects to.

For example, as a Service Now end-customer, if you upgrade to Service Now 1.3, the Service Now partner proxy that you connect to is required to be of version 1.3, 1.4, or 11.1. A Service Now partner proxy upgraded to Service Now 2.0 can only connect to end-customer Service Now applications of versions 2.0, 1.4, and 1.3.

Related Documentation

- Upgrading Junos Space Software

CHAPTER 3

Service Now Modes

- Service Now Modes on page 9

Service Now Modes

- Overview on page 9
- Activating End Customer and Partner Proxy Modes on page 11

Overview

Depending on your contract with Juniper Networks, Service Now operates in standard, end customer, and partner proxy modes. Service Now enables and disables certain features based on its mode of operation. The four modes in which Service Now operates are:

- **Demo mode**

Until you create a Service Now organization and validate the organization's connection with JSS, Service Now operates in demo mode. In demo mode, Service Now supports a single organization and up to five devices. The connection between Service Now and Juniper Support Services (JSS) is disabled, preventing creation of technical support cases.

- **Standard mode**

In standard mode, you can add multiple Service Now organizations and devices. The connection between Service Now and JSS is activated so JSS can provide support for incidents and device snapshots that you submit.

- **End customer mode**

In Service Now end customer mode, communication between Service Now and JSS is accomplished through the partner's Service Now application. A partner manages multiple end customers using a secure HTTPS connection established between the end customer's and partner's Service Now applications. Standard mode and end customer mode have similar functions; however, end customer mode limits the user to create only one organization. When an end customer uses the credentials sent by the partner to create an organization, and the organization's connection with JSS is validated, a unique ID is assigned to the end customer. To connect to the partner an end customer must specify the partner's IP address or domain on the Service Now **Global Settings** page. While incidents are submitted to JSS in standard mode, in end customer mode you submit incidents to the Service Now partner, who in turn sends

case updates back to the end customer. The partner can also submit cases to JSS on behalf of the end customer.

- **Partner proxy mode**

If you are a qualified Juniper Networks partner, you can use Service Now in partner proxy mode to manage multiple end customer Service Now applications. A secure HTTPS connection is made between the Service Now applications of every end customer and the partner, as well as between the partner and JSS. The Service Now partner receives JMBs from several end customers and can submit JMBs to JSS on behalf of the end customer or handle the cases without JSS support. To connect to an end customer, a Service Now partner uses a self-signed security certificate. Although this method of identification is not trusted, this certificate is automatically accepted to ensure that the communication between the partner and the end customer is encrypted. In partner proxy mode, you can add multiple organizations and devices groups. You associate every end customer with an organization. Cases created by end customers are opened with Juniper Networks under the site ID used for this associated organization. When you add a connected member, a default device group is created. You cannot delete this device group manually; however, it is automatically deleted when the connected member is deleted.

Table 2 on page 10 lists the tasks that are enabled for the Service Now modes.

Table 2: Tasks Enabled for Service Now Modes

Task	Demo Mode	Standard Mode	End Customer Mode	Partner Proxy Mode
Adding more than five devices	–	Enabled	Enabled	Enabled
Adding more than one organization	–	Enabled	–	Enabled
Adding connected members	–	–	–	Enabled
Updating end customer cases	–	–	–	Enabled
Assigning messages to an end customer	–	–	–	Enabled
Viewing messages assigned to an end customer	–	–	–	Enabled
Creating technical Support Cases	–	–	–	Enabled
Installing and uninstalling AI-Scripts on devices	Enabled	Enabled	–	Enabled
Other tasks	Enabled	Enabled	Enabled	Enabled

Activating End Customer and Partner Proxy Modes

End Customer Mode:

To activate end customer mode:

1. Obtain the organization credentials from the Service Now partner.
2. On the **Global Settings** page, select the **Connect to Another Junos Space** check box, enter the IP address or hostname of the partner, and click **Submit**. See “Configuring Global Settings” on page 103.
3. Add an organization using the credentials provided by the partner. See “Adding an Organization” on page 65.

End customer mode is activated.

Partner Proxy Mode:

To activate partner proxy mode:

1. On the **Manage Organizations** page in Service Now, add an organization using the credentials provided with the Service Now license.
See “Adding an Organization” on page 65.
This activates partner proxy mode, which enables you to add end customers and perform tasks that are exclusive to partner proxy mode.
2. Add connected members to Service Now.
See “Adding a Connected Member” on page 67. This enables you to manage multiple end customer Service Now applications.
3. Send the username and password that you specified in step 1 to the end customer.
The end customer uses the username and password to create an organization.

Related Documentation

- Administration Overview on page 59
- Service Central Overview on page 29
- Configuring Global Settings on page 103

CHAPTER 4

Service Now Dashboard and Workspaces Overview

- Service Now Dashboard Overview on page 13

Service Now Dashboard Overview

The Service Now dashboard displays notifications and graphically illustrates platforms and devices with most incidents. You can get to the Service Now dashboard in one of the following ways:

- Clicking **Service Now** from the Junos Space Home page.
- Selecting **Service Now** from the **Application Switcher**.
- Selecting **Home** from any page within the Service Now workspaces.



The Service Now dashboard includes:

- Service Now Workspaces on page 13
- Dashboard Gadgets on page 14

Service Now Workspaces

Apart from Service Central and Administration workspaces, Service Now also provides shortcuts to the Devices and Jobs workspaces by including them in the Service Now task ribbon. Table 3 on page 13 lists the tasks that can be performed using the Service Now workspaces.

Table 3: Service Now Workspaces

Workspace Icons	Workspace Name	Tasks
	Service Central	Manage incidents, information messages, and device snapshots; view and delete JMB errors; create and manage notification policies.
	Administration	Add and manage devices, manage script bundles and install and uninstall AI-Scripts on devices, add and manage device groups, add and manage organizations, and configure global settings.

Dashboard Gadgets

The dashboard displays gadgets with information that is updated automatically. You can move gadgets on the dashboard and change their sizes. These changes persist even after you log back in to the system. The gadgets displayed on the Service Now dashboard are:

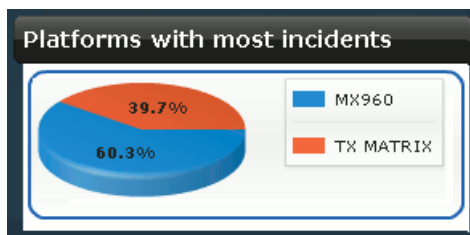
- Platforms with Most Incidents on page 14
- Devices with Most Incidents on page 14
- Service Now Notices (Upgrade and Contract Notice) on page 15

Platforms with Most Incidents

This gadget graphically displays the platforms with the most incidents along with the percentage of incidents detected on them. Clicking the elements within the graph takes you to the **Manage Incidents** page where incidents are filtered to display only the incidents that affected the platform that you clicked.

For example, when you click the **MX960** element in the **Platforms with most incidents** gadget (as shown in Figure 1 on page 14), the **Manage Incidents** page displays only those incidents that were detected on the MX960 router.

Figure 1: Platform with Most Incidents Gadget

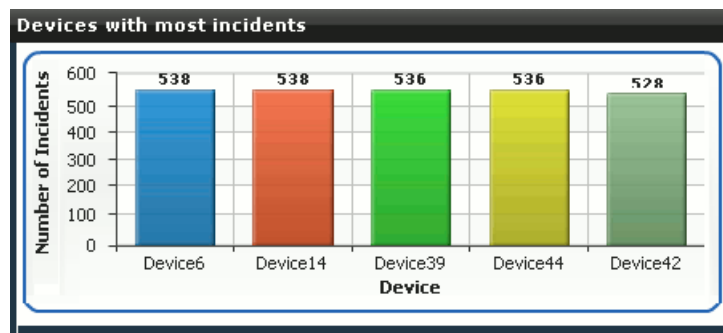


Devices with Most Incidents

This gadget graphically displays the devices with most incidents along with the number of incidents detected on them. Clicking the elements within the graph takes you to the **Manage Incidents** page where incidents are filtered, displaying only the incidents that affected the device that you selected. You can filter the incidents on the **Manage Incidents** page according to your selection on this graph. To do this, click the **Devices** bar of your choice in the graph to take you to the **Manage Incidents** page, which displays only those incidents that affect the device that you selected.

As shown in Figure 2 on page 15, clicking **Device 6**, which is represented by the blue bar of the graph, displays the **Manage Incidents** page where incidents are filtered to display only those incidents that occurred on Device 6.

Figure 2: Devices with Most Incidents Gadget

***Service Now Notices (Upgrade and Contract Notice)***

This gadget notifies you about the tasks that you need to execute subsequent to a Junos Space upgrade. It also keeps you informed about your contract with Juniper Networks.

- Related Documentation**
- Service Central Overview on page 29
 - Administration Overview on page 59
 - Service Now Icons on page 17

CHAPTER 5

Service Now Icons

- Service Now Icons on page 17

Service Now Icons

You can identify and differentiate various objects in the inventory pages of Service Now with the help of icons. These icons are displayed only in the thumbnail view of the inventory pages.

Table 4 on page 17 lists and describes the Service Now inventory page icons.

Table 4: Inventory Page Icon Description

Task	Task	Task	Icon Add-Ons	Description
Incident		Software failure incident with medium priority		Priority of the incident is critical.
		Hardware failure incident with medium priority		Priority of the incident is high.
		Resource exhaustion incident with medium priority		Priority of the incident is medium
		General Defect incident		Priority of the incident is low
				Incident case has been created.
				Incident case creation failed.
				Incident status is updated.
				End customer incident that is updated.
				End customer incident that is closed.
				

Table 4: Inventory Page Icon Description (*continued*)
















Task	Task	Task	Icon Add-Ons	Description
Tech Support cases		Technical support case		Technical support case of a connected member.
Information		Device snapshot		Device snapshot upload to JSS is successful.
				Device snapshot submission failed.
Error JMBs		JMB status: Error		
		JMB status: Invalid		
Notifications		Notification policy		A notification is sent when an incident is detected.
				A notification is sent when an incident is submitted.
				A notification is sent when a case id is assigned.
				A notification is sent when the case status is updated.
				A notification is sent when a new intelligence update is received
				The status of the reaction policy is enabled.
				The status of the reaction policy is disabled.

Table 4: Inventory Page Icon Description (*continued*)




























Task	Task	Task	Icon Add-Ons	Description
Organization		Licensed Service Now organization.		Service Now connected member or end customer.
				Unlicensed Service Now organization.
Device Group		Service Now device group		Device group of a Service Now connected member
Service Now Devices		Service Now licensed device that has no issues and does not have scripts installed.		Device has AI-Script installed.
				Device has the following issues <ul style="list-style-type: none"> • No JMBs ever sent to Service Now • Stopped sending JMBs for over two weeks. • Connection failure

Table 5 on page 20 lists and describes the Service Now task icons and the subtask icons.

Table 5: Task Icons

Workspace Name	Task Names	Task Icons	Subtask Names	Subtask Icons	Actions
Service Central	Incidents		View Tech Support Cases		Assign an owner, flag to users, update status of, delete incidents, and view a case in case manager.
			View End Customer Cases		View tech support case details and view the same in the case manager. View end customer case details and view the same in the case manager.
	Information		Messages		View and delete iJMBs, and export device data into HTML format.
			Device Snapshots		Assign an owner, flag to users, and delete information messages.
	JMB Errors		Not Applicable	Not Applicable	Download and delete JMBs that have errors.
	Notifications		Create Notifications		Create, edit, and delete notification policies.
Administration	Organization		Create Organization		Add, modify, or delete an organization. Test organization connectivity to JSS.
	Device Groups		Create Device Group		Create, modify, and delete device groups.
	Service Now Devices		Add Devices		Add devices to Service Now from the Junos Space platform. Modify and delete device parameters. Install or uninstall AI-Scripts on devices. Associate devices with device groups. Export device data into CSV and Excel format.
	Script Bundles		Add Script Bundles		Add or delete a script bundle.
	Global Settings		SNMP Settings		Configure the global settings. Add, edit, and delete SNMP Servers.
			Proxy Server Settings		Configure Proxy server settings.

- Related Documentation**
- Service Now Dashboard Overview on page 13
 - Service Now Overview on page 3

CHAPTER 6

User Roles

- Service Now User Roles on page 23

Service Now User Roles

The Junos Space User Administrator creates users and assigns roles (permissions) that allow you to access and perform different tasks. You cannot view the tasks that you do not have access to. While Junos Space enables you to create users with custom permissions, it also has a set of predefined user roles. You cannot modify or delete these predefined roles. See Table 6 on page 24, which describes the tasks that predefined Service Now users have access to, based on the roles assigned to them.

You can create users and manage them on the **Manage Users** page, if you have User Administrator permissions. To create and manage these users, select **Application Switcher > Network Application Platform > Users > Manage Users**. The **Manage Users** page lists the existing users. Use this page to create and assign roles to Service Now users.

You can also navigate to the **Manage Users** page by selecting **Application Switcher > Jump to Users**.

Table 6: Predefined Service Now User Roles and Permissions

Role	Permitted to Execute Actions Under the Following Subtasks	
Service Now Admin	Administration	Service Now Devices, New Device Platform. Event Profiles, Add Event Profile. Script Bundle, Add Script Bundle. Organization, Add Organization. Global Settings, SNMP Configuration, Proxy Server Configuration. Device Group, Create Device Group.
	Service Central	Incidents, View Tech Support Cases. JMB Errors Information, Messages, Device Snapshots. Notifications, Create Notification.
Service Now Unrestricted User	Administration	Service Now Devices
	Service Central	Incidents, View Tech Support Cases. JMB Errors Information, Messages, Device Snapshots. Notifications, Create Notification. Permissions exclude the ability to delete managed objects.
Service Now Read Only User	Administration	Viewing and exporting Service Now devices
	Service Central	Viewing JMB details Exporting incident summary into an Excel format Viewing an incident case in the case manager Viewing a technical support case in case manager View end customer cases in case manager Downloading JMB errors Scanning an information message for impact Exporting a JMB (device snapshot) to HTML. Viewing JMB (device snapshot) details Viewing notification policies

Incidents can be flagged or assigned only to a Service Now Admin or Service Now Unrestricted User. An information message or iJMB can be flagged or assigned to any user. Every user has the ability to clear a flag of an incident or information message that was flagged to that user.

Related Documentation

- Administration Overview on page 59

PART 2

Using the Service Now Getting Started Assistant

- Service Now Getting Started Assistant Usage Overview on page 27

CHAPTER 7

Service Now Getting Started Assistant Usage Overview

- Service Now Getting Started Assistant Usage Overview on page 27

Service Now Getting Started Assistant Usage Overview

The Getting Started assistant is a panel in the Junos Space sidebar that guides you through the tasks that you can perform as part of the initial setup for every application. It is displayed when you log in to Junos Space and the **Show Getting Started on Startup** check box is selected.

To use the Service Now Getting Started assistant, navigate to Service Now, click the **Help** icon, expand the **Getting Started** assistant, and click the **Initial Setup** link. The **Getting Started** assistant displays five required steps and one optional step.

Every step in the Getting Started assistant contains a task link, and alongside the task links are help icons that provide information about the individual tasks. To execute the steps, click the task links of every step. The inventory page displays the page where you can execute the tasks.

By default, the **Getting Started** assistant guides you through the steps required to set up standard mode for Service Now.

The following steps are required:

1. Review Global Settings.
See "Configuring Global Settings" on page 103
2. Create Organization.
See "Adding an Organization" on page 65.
3. Add Devices to Junos Space.
See the *Discovering Devices* section from the *Network Application Platform User Guide*.
4. Create Device Group.
See "Creating a Device Group" on page 73.
5. Install Scripts using Service Now Devices.
See "Installing an Event Profile on Devices Using Service Now" on page 80

The following step is optional:

- Add New Script Bundle.
See “Adding a Script Bundle to Service Now” on page 99.

To activate Service Now in end customer and partner proxy modes, see the *Activating the End Customer and Partner Proxy Modes* section in “Service Now Modes” on page 9.

**Related
Documentation**

- Service Now Overview on page 3

PART 3

Service Central

- Service Central Overview on page 29
- Incidents on page 31
- Information on page 41
- JMB Errors on page 49
- Notifications on page 51

Service Central Overview

The Service Central workspace is a Service Now module that enables you manage incidents, information messages, device snapshots, and error JMBs. Incidents are problem events that are detected in a device and sent to the Service Now application. When an event occurs on a device, AI-Scripts installed on the device create files called Juniper Message Bundles (JMBs) that contain comprehensive information about the device identity, the problem event, and diagnostics. The JMB file is then transferred securely from the device to Service Now. Service Now searches for new incidents and displays the incidents on the **Manage Incidents** page.

After reviewing an incident, you can use the Incidents task to submit an incident case to the Juniper Support Systems (JSS) to create a Juniper Networks Technical Assistance Center (JTAC) case. You can notify users of the incident, assign a user as an owner of the incident, and delete the incident from the platform.

In addition to reporting incidents, AI-Scripts also send device information regularly to Service Now in the form of Information Juniper Message Bundles (iJMBs). The iJMBs are then processed and displayed on the **Manage Device Snapshots** page. You can upload these iJMBs to JSS, where they are processed and analyzed to provide preventive analysis and alerts. Using Service Now, you can view the content of these iJMBs and export them in HTML format.

JMB errors are JMBs that do not comply with the standard data structure that Service Now requires or that contain data elements that Service Now does not accept. Service Now identifies these JMBs and displays them on the **Manage JMB Errors** page where you can be view and download them.

You can use a notification policy to specify the events for which you want to receive a notification. The options are New Incident Detected, Case Submitted, Case Status Updated, and Intelligence Update Received. Notification policies define other characteristics (filters) that you can use to fine tune the conditions under which you

receive a notification. You can even define the events that trigger the notification, the filters that further specify the trigger events, and the actions that you want Service Now to take after the event is triggered.

Some tasks within the Service Central workspace, such as assigning messages to a connected member and updating an end customer case, are enabled only when the Service Now end customer mode is activated. For more information on the Service Now modes, see “Service Now Modes” on page 9.

The **Service Central** page graphically displays information about the severity and priority of incidents and the incidents you created.

Using Service Central you can perform the following tasks:

- Assign an incident owner, flag incident to users, update status of, and delete incidents.
- View and delete iJMBs, and export device data into HTML format.
- Assign messages to end customers (enabled if you are a Service Now partner).
- Update end customer cases (enabled if you are a Service Now partner).
- View, download, and delete JMBs with errors.
- Assign an owner, flag to users, and delete an information message.
- Create, edit, and delete a notification policy.

**Related
Documentation**

- Service Now Overview on page 3
- Service Now Modes on page 9
- Incidents Overview on page 31
- Device Snapshots Overview on page 45
- Messages Overview on page 41
- JMB Errors on page 49
- Notification Policies Overview on page 51

CHAPTER 8

Incidents

- Incidents Overview on page 31
- Assigning an Incident Owner on page 32
- Flagging an Incident to a User on page 33
- Checking Incident Status Updates on page 34
- Exporting Incident Data on page 34
- Deleting an Incident on page 35
- Submitting an Incident to Juniper Support Systems on page 36
- Viewing Incident Details on page 36
- Viewing a Case in the Case Manager on page 37
- Modifying Submit Case Options on page 38
- Updating an End Customer Case on page 39

Incidents Overview

In Service Now, incidents are problem events that are detected on a device. When an incident, such as a process crash, an application-specific integrated circuit (ASIC) error, or a fan failure, occurs on an AI-Scripts-enabled device, the AI-Script builds a JMB file with the incident data and forwards it to the Junos Space server. AI-Scripts create files called Juniper Message Bundles (JMBs).

A JMB file is an XML file that contains diagnostic information about the device and other information specific to the condition that triggered the event message. The incident contains information such as hostname, time stamp of the incident, synopsis, description, chassis serial number of the device, and the severity and priority of the incident.

These JMB files are securely transferred from the device to the Service Now application. After a JMB is generated, the device automatically initiates a file transfer to Service Now and the incident is displayed on the **Manage Incidents** page.

Service Now uses Device Management Interface (DMI), which is an extension to the NETCONF network management protocol, to receive JMBs from devices. The **Manage Incidents** page provides a user interface to view incidents chronologically, by organization name, and by device group. The thumbnail view of this page helps you differentiate

incidents with various icons. These icons indicate incident priority levels and also whether the incidents are submitted to JSS. See “Service Now Icons” on page 17.

From the Incidents workspace you can navigate to the **View Tech Support Cases** and **View End Customer Cases** pages. The **View Tech Support Cases** page displays the technical support cases that you open with JSS. You can open these cases only after you create an organization and the organization's site ID is validated. Site IDs denote the customer identity used in the Juniper Networks Technical Assistance Center (JTAC) Clarify trouble ticketing system.

To stay updated of the events that occur in Service Now, you can create notification policies that instantly notify you of an event in the form of e-mails or SNMP traps.

You can display incidents either as thumbnails or arranged in a table. If you choose to display incidents in a table, the **Manage Incidents** page lists them by incident ID, organization, device group, defect type, platform type, time of occurrence, owner, submission status, and incidents that are flagged to you. You can select which parameters to display and sort them in the ascending or descending order.

You can perform the following tasks from the **Manage Incidents** page:

- Submit an incident to create a JTAC case
- Flag the incident to another user
- Assign the incident to another user
- Delete an incident
- View the details of a Juniper Message Bundle (JMB)
- View a case in the Juniper Networks Case Manager
- Remove a flag from the incident
- Add an e-mail address to the mailing list of an incident
- View tech support cases

Related Documentation

- Assigning an Incident Owner on page 32
- Flagging an Incident to a User on page 33
- Deleting an Incident on page 35

Assigning an Incident Owner

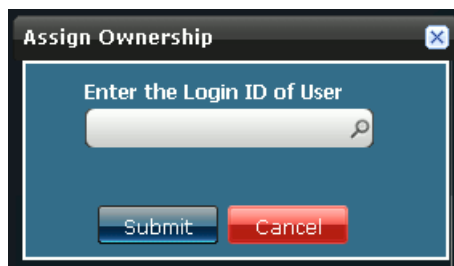
You can assign an incident to a Junos Space user, who becomes the owner of the incident. The owner is responsible for keeping track of the progress of a case or updates from JSS.

To assign an incident to a Service Now user:

1. From the Service Now task ribbon, select **Service Central > Incidents**.
The **Manage Incidents** page is displayed.
2. Select the incident for which you want to assign an owner.

3. Select **Assign Ownership** from the Actions panel.

The **Assign Ownership** dialog box is displayed.



4. Enter the login ID of the user to whom you want to assign the incident. Click the search icon to display the list of available users.
5. Click **Submit**.

The incident is assigned to the specified user. See “Viewing Device Snapshot Details” on page 46

- Related Documentation**
- Incidents Overview on page 31
 - Flagging an Incident to a User on page 33

Flagging an Incident to a User

You can flag an incident to a user who might be affected by the incident or needs to be aware of updates to it. When changes are made to this incident, the user receives an e-mail. If an incident is flagged to you, the Flag column of that incident in the Incidents table displays **Yes**. If not, it displays **No**.

To flag an incident to a user:

1. From the Service Now task ribbon, select **Service Central > Incidents**.
The Manage Incidents table is displayed.
2. Select the incident that you want to flag to a user.
3. Select **Flag to Users** from the Actions panel.
The **Flag to Users** dialog box displays the names of Service Now users.
4. Select the user or users to whom you want to flag the incident.
5. Click **Submit**. The incident is flagged to the selected users.

- Related Documentation**
- Incidents Overview on page 31
 - Assigning an Incident Owner on page 32

Checking Incident Status Updates

In Service Now, incidents are problem events that are detected in a device. Information about these incidents is sent to the Service Now application. Service Now routinely checks for new incidents. The Service Now **Manage Incidents** page provides a user interface to view incidents chronologically by organization name and device group.

You can use the **Manage Incidents** page to submit an incident so that a Juniper Networks Technical Assistance Center (JTAC) case is created. The submission status of the incident is displayed in the Status column on the **Manage Incidents** page. After you submit the incidents, the status is **Submitted**. When JSS creates the case, the status changes to **Created** and the Case ID appears. Further updates to the incident change the incident's status to **Updated**.

Service Now provides three ways to check incident status.

- Using Junos Space logs. The Junos Space log of an incident displays a list of the status changes.
- Using notification policies. You can create a notification policy to notify users whenever the status of an incident is updated. For more information about creating notification policies, see "Creating and Editing a Notification Policy" on page 52.
- Using the Service Central page. The My Incidents graph on the Service Central page displays the number of incidents whose status has changed since you last logged in. It also displays other information such as the number of incidents that were flagged to you, the number of incidents that you own, and the number of new incidents that were added since your last login. To view the Service Central page, select **Service Central** from the Service Now task ribbon.

Related Documentation

- Incidents Overview on page 31
- Assigning an Incident Owner on page 32

Exporting Incident Data

You can export incident data into HTML and Excel file formats and save it on your local file system.

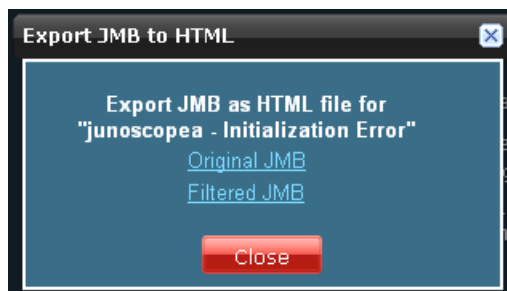
Exporting Incident Data into HTML

To export incident data into HTML format:

1. From the Service Now task ribbon, select **Service Central > Incidents**.
The **Manage Incidents** page is displayed.
2. Select the device whose incident details you want to export.
3. Select **Export JMB to HTML** from the Actions panel.

The **Export JMB to HTML** dialog box displays links to the original and filtered JMBs, as shown in Figure 3 on page 35.

Figure 3: Export JMB to HTML Dialog Box



4. Click a link to save the JMB file as HTML.

Exporting Incident Data into Excel

To export JMB data into Excel file format:

1. From the Service Now task ribbon, select **Service Central > Incidents**.

The **Manage Incidents** page is displayed.

2. Select the incident whose details you want to export.
3. Select **Export Incident Summary to Excel** from the Actions panel.

The **Export Incident Summary to Excel** dialog box displays a link to the Excel file.

4. Click the displayed link to save the incidents in Excel format

Related Documentation

- Incidents Overview on page 31
- Assigning an Incident Owner on page 32
- Flagging an Incident to a User on page 33

Deleting an Incident

After reviewing the incident information, you can use the **Manage Incidents** page to delete incidents from Service Now. This action deletes the incident both from the Service Now database and from the Incidents table.

To delete an incident:

1. From the Service Now task ribbon, select **Service Central > Incidents**.

The Incidents table is displayed.

2. Select the incident that you want to delete.
3. Click **Delete**.

The selected incidents are removed from the Incidents table and the Service Now database.

Related Documentation

- Incidents Overview on page 31

- Flagging an Incident to a User on page 33

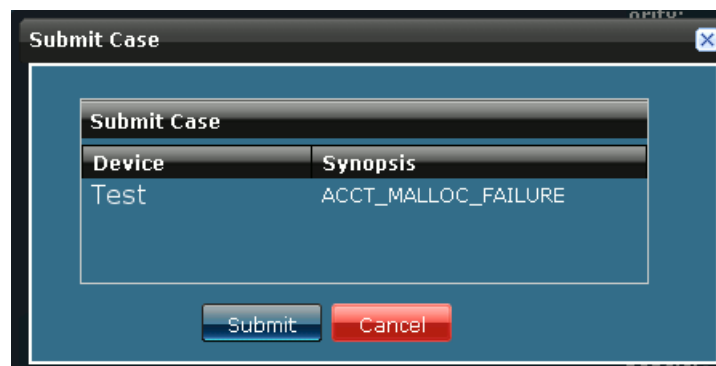
Submitting an Incident to Juniper Support Systems

After reviewing the incident information, you can use the **Manage Incidents** page to submit an incident to create a case. You can submit multiple cases to Juniper Support Systems (JSS) simultaneously. The submission status of the incident is displayed in the **Status** column on the **Manage Incidents** page. After you submit the incident, the status is **Submitted**. When the case is created by JSS, the status changes to **Created** and the Case ID appears.

To submit an incident:

1. From the Service Now task ribbon, select **Service Central > Incidents**.
The **Manage Incidents** page is displayed.
2. Select the incident for which you want to create a case.
3. Select **Submit Case** from the Actions panel.

The **Submit Case** dialog box displays the device name, and incident synopsis. The **Submit Case** action is disabled when you select an incident that is already submitted.



4. Click **Submit** to submit the case to create a JTAC.

The **Manage Incidents** page displays the submission status in the Status column. Thereafter, the status is **Submitted**. When the case is created by JSS, the status changes to **Created** and the Case ID appears.

- Related Documentation**
- Incidents Overview on page 31
 - Flagging an Incident to a User on page 33

Viewing Incident Details

When incidents are received, only selected information is displayed on the **Manage Incidents** page. Using Service Now, you can view the entire content of the incident.

To view incident details:

1. From the Service Now task ribbon, select **Service Central > Incidents**.

The **Manage Incidents** page is displayed.

2. Select the incident whose details you want to view.

3. Select **View JMB** from the Actions panel.

The **View JMB** dialog box displays links to the original and filtered JMB details.

4. Click the link.

This new window displays the details of the selected incident.

- Related Documentation**
- Incidents Overview on page 31
 - Flagging an Incident to a User on page 33

Viewing a Case in the Case Manager

You can view the details of a submitted case in the Juniper Networks Case Manager. To view case details in the Case Manager, you must first have a user Id and password for the Juniper Networks Customer Support Center (CSC). You can request the user Id and password at <http://www.juniper.net/customers/support/> or by contacting Juniper Networks Customer Care.

To view a case in the Case Manager:

1. From the Service Now task ribbon, select **Service Central > Incidents**.

The **Manage Incidents** page is displayed.

2. Select the incident whose details you want to view in the Case Manager.

3. Select **View Case in Case Manager** from the **Actions** panel.

If the **View Case in Case Manager** link is not enabled, ensure that the case has been created. The Juniper Networks Login page is displayed.

4. Enter your user name and password and click **Login**.

The JSS Case Manager displays the case details.



NOTE: You can also view the details of the submitted cases in the Case Manager from the **View Tech Support Cases** page. To view case details, go to **Service Central > Incidents > View Tech Support Cases** and follow steps 2, 3, and 4 from the preceding procedure.

- Related Documentation**
- Incidents Overview on page 31
 - Flagging an Incident to a User on page 33

Modifying Submit Case Options

For any incident in Service Now, you can modify the submit case settings, such as the case priority and the e-mail list associated with the case. You can also add your comments to the synopsis and the description of an incident before you submit it to Juniper Support Systems (JSS).

To modify submit case options:

1. From the Service Now task ribbon, select **Service Central > Incidents**.

The Incidents table is displayed.

2. Select the incident whose submit case options you want to modify.
3. Select **Modify Submit Case Options** from the Actions panel.

The **Modify Submit Case Options** dialog box is displayed.

Modify Submit Case Options

Add CC to Case:

Add Email Delete

Email List	Enter Email Id

Priority:

High

Synopsis:

RPD_ISIS_OVERLOAD

Add Comments to Synopsis:

Problem Description:

RPD_ISIS_OVERLOAD: No additional memory is available for storing IS-IS link-state information. Either system resources are exhausted or a software error occurred (such as a memory leak in the routing protocol process [rpd]).

Add Comments to Description:

Save Save And Submit Cancel

4. Use the **Enter Email Id** check box to enter an e-mail ID.

Enter the e-mail ID in the format user@example.com. To add multiple e-mail IDs, and delete, use the **Add Email** and **Delete** buttons respectively.

5. Select one of the options from the **Priority** list to modify the priority of the case. The available options are Critical, High, Medium, and Low. The default priority is medium.

6. To add your comments to the problem description and synopsis of the case, enter your comments in the **Add Comments to Synopsis** and **Add Comments to Description** fields.

The maximum limit for the comments is 1028 characters.

7. To save your settings in the Service Now database, click **Save**.

Your settings are saved and the **Manage Incidents** page is displayed.

8. To save your settings in the Service Now database and submit the selected incident to JSS, click **Save and Submit**.

The incident is submitted to JSS and your settings are saved in the Service Now database. You are taken to the **Manage Incidents** page.

Related Documentation

- Incidents Overview on page 31
- Submitting an Incident to Juniper Support Systems on page 36

Updating an End Customer Case

As a Service Now partner, you can create a case for the incident you receive from an end customer's device and also update the case.



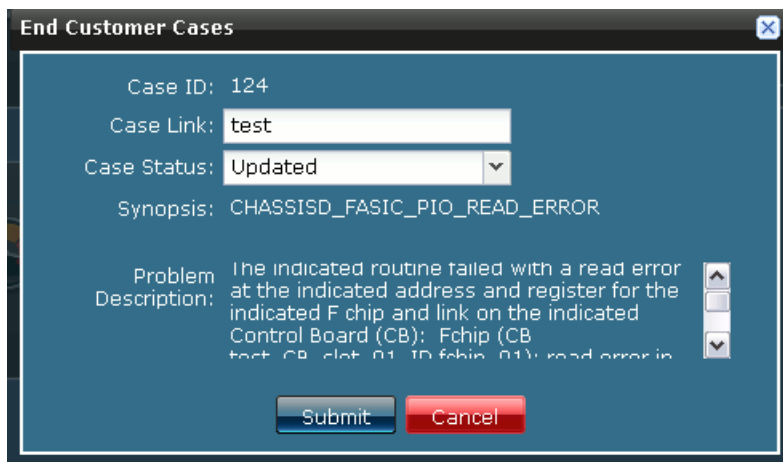
NOTE: This action is enabled only when Service Now operates in partner proxy mode and when the state of the selected case is open.

To update an end customer case:

1. From the Service Now task ribbon select, **Service Central > Incidents**.
The **Manage Incidents** page displays the list of incidents.
2. Select the end customer incident for which you want to create a case.
3. Right-click your selection and select **End Customer Case**.

The **End Customer Case** dialog box is displayed as shown in Figure 4 on page 40.

Figure 4: End Customer Cases Dialog Box



The dialog box is titled "End Customer Cases" and contains the following fields and controls:

- Case ID:** 124
- Case Link:** test
- Case Status:** Updated (with a dropdown arrow)
- Synopsis:** CHASSISD_FASIC_PIO_READ_ERROR
- Problem Description:** The indicated routine failed with a read error at the indicated address and register for the indicated F chip and link on the indicated Control Board (CB): Fchip (CB test CB slot 01 ID fchip 01): read error in
- Buttons:** Submit and Cancel

You can also select **End Customer Case** from the **Actions** panel.

This **End Customer Case** action is enabled only if you select an end customer incident.

4. Modify the case details.
5. Click **Submit**.

The case is updated and sent to the Service Now end customer.

- Related Documentation**
- Service Now Overview on page 3
 - Adding a Connected Member on page 67

CHAPTER 9

Information

- Messages Overview on page 41
- Assigning Ownership on page 42
- Flagging a Message to Users on page 42
- Deleting a Message on page 43
- Scanning a Message for Impact on page 43
- Assigning a Message to a Connected Member on page 43
- Device Snapshots Overview on page 45
- Exporting Device Data into HTML on page 45
- Deleting Device Snapshots on page 46
- Viewing Device Snapshot Details on page 46

Messages Overview

Service Now polls Juniper Support Systems (JSS) regularly to receive information messages for every configured organization. These information messages are displayed on the Service Now **Manage Messages** page. Using Service Now, you can assign every information message to an owner and flag it to users. This ensures that users are kept informed of changes made to information messages.

You perform the following tasks using the Information Messages tab:

- Assigning an information message owner
- Flagging an information message to users
- Deleting information messages
- Scanning for affected devices

Related Documentation

- Device Snapshots Overview on page 45
- Assigning Ownership on page 42
- Flagging a Message to Users on page 42
- Scanning a Message for Impact on page 43
- Deleting a Message on page 43

Assigning Ownership

You can assign every information message to a Junos Space user who needs to be notified.

To assign an owner (Junos Space user) to an information message:

1. From the Service Now task ribbon, select **Service Central > Information > Messages**.
The **Manage Messages** page is displayed.
2. Select the information message to which you want to assign an owner.
3. Select **Assign Ownership** from the Actions panel.
The **Assign Ownership** dialog box is displayed.
4. Enter the Login ID of the Junos Space user.
5. Click **Submit**.

The specified user is assigned ownership of the selected information message.

- Related Documentation**
- Device Snapshots Overview on page 45
 - Flagging a Message to Users on page 42

Flagging a Message to Users

You can flag an information message to a Junos Space user who you think needs to keep track of the information message or who needs to be notified when it is changed.

To flag an information message to a user:

1. From the Service Now task ribbon, select **Service Central > Information > Messages**.
The Messages page is displayed.
2. Select the information message that you want to flag to a user.
3. Select **Flag to Users** from the Actions panel.
The **Flag to Users** dialog box lists the available users.
4. Select one or more users who must be notified of the selected information message.
5. Click **Submit**.

The specified users are notified of the selected information message. The selected information message are flagged to them, and the **Flag** column of that information message displays **Yes**.

- Related Documentation**
- Device Snapshots Overview on page 45
 - Messages Overview on page 41

Deleting a Message

You can delete information messages from the Service Now database that Service Now collects and that are displayed on the **Manage Messages** page.

To delete an information message:

1. From the Service Now task ribbon, select **Service Central > Information > Messages**.

The **Manage Messages** page is displayed.

2. Select the information message that you want to delete.
3. Select **Delete** from the Actions panel. Click **Delete** again to confirm deletion.

The selected information messages are deleted from the Service Now database and they no longer appear on the **Manage Messages** page.

- Related Documentation**
- Device Snapshots Overview on page 45
 - Messages Overview on page 41

Scanning a Message for Impact

You can use Service Now to view the devices impacted by the vulnerabilities described in the inform message.

To scan iJMBs and view the impacted devices:

1. From the Service Now task ribbon, select **Service Central > Information > Messages**.

The **Manage Messages** page is displayed.

2. Select the message that you want to scan for impact.
3. Select **Scan for Impact** from the Actions panel.

The **Scan for Impact Results** page displays the list of devices that are impacted by the selected message. If no devices are impacted by the selected message, the following message is displayed:

No impacted devices found.

- Related Documentation**
- Messages Overview on page 41
 - Viewing Device Snapshot Details on page 46

Assigning a Message to a Connected Member

Service Now polls JSS regularly to receive messages for every configured organization. As a Service Now partner, you can assign multiple messages to a connected member. This action is available only when Service Now operates in partner proxy mode. For more

information about standard, partner, and end customer modes, see “Service Now Modes” on page 9.



NOTE: After a message is assigned to a Connected Member it cannot be deleted.

To assign a message to a connected member:

1. From the Service Now task ribbon, select **Service Central > Information > Messages**.
The **Manage Messages** page displays the list of information messages received.
2. Select the message that you want to assign to a connected member.
3. Right-click your selection or use the **Actions** panel and select **Assign Message to End Customer**.

As shown in Figure 5 on page 44, the **Choose Connected Members** dialog box displays the list of connected members and also the connected members to whom the message is already assigned along with the status.

Figure 5: Choose Connected Members Dialog Box

Site Name	Status	Sent
Test	Delivered	2010/05/07 09:13

Warning: Messages once assigned to a Connected Member cannot be deleted.

4. Select the connected member to whom this message can be assigned.
5. Click **Submit**.

The selected message is assigned to the connected member. To verify this action you can navigate to the **Manage Organizations** page, and list the messages assigned to any connected member. See “Viewing Messages Assigned to a Connected Member” on page 70.

Related Documentation

- Adding a Connected Member on page 67

Device Snapshots Overview

Service Now periodically collects and displays Information Juniper Message Bundles (iJMBs) that contain information about devices. These iJMBs are processed and displayed on the **Manage Device Snapshot** page in the Service Now application. You can upload these iJMBs to JSS, where they are added to the Customer Intelligence Database (CIDB) database, and then processed and analyzed to provide preventive measures.

You can also filter the configuration content from an iJMB before sending it to JSS, with the help of Service Now global settings, and then track the status of the iJMB submission to JSS.

Devices that have stopped sending information (device snapshots) to Service Now for more than two weeks are also detected and graphically displayed on the Administration page. To list these devices you can click the **Devices Not Sending Snapshots** bar of the **Devices Not Sending Device Snapshots** graph. These devices are displayed on the **Service Now Devices** page where you can view their details and export them to HTML format. The thumbnail view of the **Manage Device Snapshots** page uses different icons to help you identify snapshots that have been successfully uploaded to JSS and the device snapshots whose submission to JSS failed. For a description of these icons, see “Service Now Icons” on page 17.

You perform the following tasks using the Information Device Snapshots tab:

- Exporting Device Data into HTML
- Deleting an iJMB
- Viewing iJMB Details

Related Documentation

- Exporting Device Data into HTML on page 45
- Viewing Device Snapshot Details on page 46
- Messages Overview on page 41

Exporting Device Data into HTML

You can take device data that Service Now collects and displays on the **Manage Device Snapshots** page and export it in HTML format.

To export device data in HTML format:

1. From the Service Now task ribbon, select **Service Central > Information > Device Snapshots**.

The **Manage Device Snapshots** page displays the device snapshots received.

2. Select the organization whose data you want to export.
3. Select **Export to HTML** from the **Actions** panel.

The **Export JMB to HTML** dialog box displays links to the original and filtered versions of the JMB.

4. Click the displayed link to save the iJMB as HTML.

**Related
Documentation**

- Messages Overview on page 41
- Viewing Device Snapshot Details on page 46

Deleting Device Snapshots

You can take device data that Service Now collects and displays on the **Manage Device Snapshots** page and delete it from the Service Now database.

To delete an iJMB:

1. From the Service Now task ribbon, select **Service Central > Information > Device Snapshots**.

The **Manage Device Snapshots** page is displayed.

2. Select the organization whose device information you want to delete.
3. Select **Delete** from the Actions panel.

The **Delete Device Snapshots** dialog box asks you for a confirmation.

4. Click **Delete** to confirm deletion.

The iJMBs from the selected organizations are deleted from the Service Now database and they no longer appear on the **Manage Device Snapshots** page.

**Related
Documentation**

- Messages Overview on page 41
- Viewing Device Snapshot Details on page 46

Viewing Device Snapshot Details

When Service Now receives iJMBs, only selected information is displayed on the **Manage Device Snapshots** page. You can display the entire content of the iJMB using the View JMB action in Service Now.

To view the details of an iJMB:

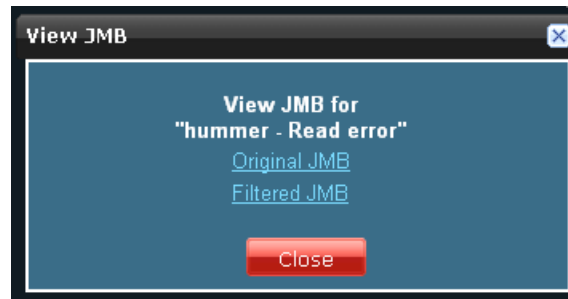
1. From the Service Now task ribbon, select **Service Central > Information > Device Snapshots**.

The **Manage Device Snapshots** page is displayed.

2. Select the organization whose iJMB contents you want to view.
3. Select **View JMB** from the **Actions** panel.

The **View JMB** dialog box displays links to the original and the filtered iJMBs as shown in Figure 6 on page 47. The information in the filtered JMB is classified by the settings on your **Global Settings** page.

Figure 6: View JMB Dialog Box



4. Click a link.

A new window displays the iJMB details.

Related Documentation

- Messages Overview on page 41

CHAPTER 10

JMB Errors

- JMB Errors on page 49

JMB Errors

Service Now identifies the Juniper Message Bundles (JMBs) with errors and displays them on the **Manage JMB Errors** page for monitoring purposes. You can download up to five JMB files at a time and also delete them from the Service Now database. JMBs with errors are JMBs that do not comply with the standard data structure or other data elements that Service Now accepts. We recommend that you open a case with JSS for unique error JMBs.

- Downloading JMB Errors on page 49
- Deleting JMB Errors on page 50

Downloading JMB Errors

To download the JMB errors in a zipped file:

1. From the Service Now task ribbon, select **Service Central > Incidents > JMB Errors**.

The **Manage JMB Errors** page is displayed.



2. Select the JMB whose details you want to download. You can download up to five JMB files at a time.
3. Select **Download JMB Errors** from the Actions panel.

The **Download JMB Errors** dialog box is displayed.

4. Click the **Click here to download JMB Error files** link to save the selected JMB in a zipped file.

Deleting JMB Errors

To delete an error JMB:

1. From the Service Now task ribbon, select **Service Central > Incidents > JMB Errors**.

The **Manage JMB Errors** page is displayed.

2. Select the JMB that you want to delete.
3. Select **Delete** from the Actions panel.

The **Delete Error JMB** dialog box prompts you to confirm the deletion.

4. Click **Delete**.

The selected error JMBs are deleted from the Service Now database and they no longer appear on the **Manage JMB Errors** page.

- Related Documentation**
- Service Central Overview on page 29
 - Messages Overview on page 41

CHAPTER 11

Notifications

- Notification Policies Overview on page 51
- Creating and Editing a Notification Policy on page 52
- Enabling or Disabling a Notification Policy on page 57
- Deleting a Notification Policy on page 57

Notification Policies Overview

In Service Now, a notification policy specifies the events for which you want Service Now to send a notification and also for the actions you want taken. Service Now sends you a notification when a specific event occurs. Notification policies define the parameters for these notifications.

You can specify the following parameters when you create a notification policy

- Trigger—Specify the event that causes Service Now to send the notification.
- Filters—Further specify the events that cause Service Now to send a notification.
- Actions—Specify the action (or actions) that must be taken after the specified event is triggered. These events can be filtered by priority, device name, serial number, and so on. Different filters are supported for incident and information trigger types.

Service Now provides an interface where you can manage these notification policies. The **Manage Notifications** page displays the notification policies chronologically by name, owner, status, and trigger. For more information about the Manage Notifications table columns, see Table 7 on page 51.

Table 7: Notification Policies Table Column Descriptions

Element Name	Description	Privilege Required to Modify	Range/Length	Default
Name	Name of the policy, which must be unique among all policies owned by the same user	Hyperlink requires Notification Policy privilege	64 characters	Not applicable
Owner	Name of the user who owns the notification policy	Not applicable	Not applicable.	Not applicable

Table 7: Notification Policies Table Column Descriptions (*continued*)

Element Name	Description	Privilege Required to Modify	Range/Length	Default
Status	Whether the notification policy is running	Not applicable	Enabled or Disabled	Not applicable
Trigger Type	Type of the trigger for which the notification policy is applied	Not applicable	<ul style="list-style-type: none"> New Incident Detected Incident Submitted Case ID Assigned Case Status Updated New Intelligence Update 	Not applicable

- Related Documentation**
- Creating and Editing a Notification Policy on page 52
 - Enabling or Disabling a Notification Policy on page 57
 - Deleting a Notification Policy on page 57

Creating and Editing a Notification Policy

Notification policies specify when you want Service Now to send notifications, and also who to send the notifications to. You can define the events that trigger the notification, the filters that further specify the trigger events, and the actions that you want Service Now to take after the event is triggered. You can also choose to attach or discard the JMB files that are sent along with the e-mail notifications.

To create a notification policy:

1. From the Service Now task ribbon, select **Service Central > Notifications > Create Notifications**.

The **Service Central: Create Notifications** page is displayed as shown in Figure 7 on page 53.

Figure 7: Create Notifications dialog box

2. Enter a notification policy name and select a trigger.
3. Enter the filter parameters.
Different filters are supported for incident and information trigger types.
4. Enter the e-mail IDs of users to whom the notification must be sent.

For more information about the fields in the **Create Notification Policy** dialog box, see Table 8 on page 54.

5. (Optional) If you do not want to attach the JMB files in the e-mails sent as notifications, uncheck the **Send JMB file as attachment in mail** check box.
6. Click **Add**.

The notification policy is created and displayed on the **Manage Notifications** page.

Copying a notification policy

You can also copy an existing notification policy and modify its attributes to create another notification policy.



NOTE: While copying a notification policy, you cannot edit the **Trigger** field.

To copy a notification policy:

1. From the Service Now task ribbon, select **Service Central > Notifications**.

The **Manage Notifications** page is displayed.

2. Select the notification policy that you want to copy.
3. Select **Copy** from the Actions panel.

The **Service Central: Notifications** page is displayed.

4. Make your modifications.
5. Click **Make a Copy**.

A notification policy is created with the settings that you specified.

Editing a notification policy

To modify a notification policy:

1. From the Service Now task ribbon, select **Service Central > Notifications**.

The **Manage Notifications** page is displayed.

2. Select the notification policy that you want to edit.
3. Select **Edit filters and Actions** from the Actions panel.

The **Edit Notifications** page is displayed.

4. Edit the required fields.

See Table 8 on page 54, and for more information see Table 9 on page 56.

Table 8: Create Notification Policy Page Field Descriptions

Field	Description	Range/Length	Default
Name	Type the name of the policy, which must be unique to the policies a user owns.	64 characters	Not applicable

Table 8: Create Notification Policy Page Field Descriptions (*continued*)

Field	Description	Range/Length	Default
Trigger Type	Type the type of trigger required to activate this policy. The fields in the filter table dynamically change according to the selected trigger type.	<ul style="list-style-type: none"> • New Incident Detected • Incident Submitted • Case ID Assigned • Case Status Updated • New Intelligence Update 	Not applicable
Apply Filters:			
Common Filter Parameters:			
Priority	Select a value in the Priority field. Service Now sends a notification if the priority of the incident matches the entered value. Regular expressions can also be used in this field.	255 characters	Blank
Device Name	Type a value in the Device Name field. Service Now sends a notification if the name of the device the incident occurred on matches the entered value. Regular expressions can also be used in this field.	255 characters	Blank
Serial Number	Type a value in the Serial Number field. Service Now sends a notification if the serial number of the device the incident occurred on matches the entered value. Regular expressions can also be used in this field.	255 characters	Blank
Has the words	Type a value in the Has the words field. Service Now sends a notification if the specified words match any of the fields in the incident or the information message. Regular expressions can also be used in this field.	255 characters	Blank
Does not have	Type a value in the Doesn't have field. Service Now sends a notification if the specified words do not match any of the fields in the incident or the information message. Regular expressions can also be used in this field.	255 characters	Blank
Information Trigger Type Notification Policy Filter Parameters:			
Intelligence Update Type	Type a value in the Intelligence Update Type field. Service Now sends a notification if the type of information message update matches the entered value.	255 characters	Blank
Products Affected	Type a value in the Products Affected field. Service Now sends a notification if the Products Affected field value in alert information messages matches the entered value	255 characters	Blank
Platform Type	Type a value in the Platform Type field. Service Now sends a notification if the Platforms Affected field in alert information messages or the platform type field in information messages match the entered value	255 characters	Blank
Keywords	Type a value in the Keywords field. Service Now sends a notification if the Keyword in information messages matches the entered value	255 characters	Blank

Table 8: Create Notification Policy Page Field Descriptions (*continued*)

Field	Description	Range/Length	Default
Serial Number	Type a value in the Serial Number field. Service Now sends a notification if the serial number of the device the incident occurred on matches the entered value. Regular expressions can also be used in this field.	255 characters	Blank
Software Version	Type a value in the Software Version field. Service Now sends a notification if the software version in the information messages matches the entered value	255 characters	Blank
Devices Impacted	Type a value in the Devices Impacted field. Service Now sends a notification if the devices impacted in the information messages matches the entered value	255 characters	Blank
Has the words	Type a value in the Has the words field. Service Now sends a notification if the specified words match any of the fields in the incident or the information message. Regular expressions can also be used in this field.	255 characters	Blank
Does not have	Type a value in the Doesn't have field. Service Now sends a notification if the specified words do not match any of the fields in the incident or the information message. Regular expressions can also be used in this field.	255 characters	Blank
Actions:			
Send Email to	<p>Type the e-mail addresses of users who must receive an alert if the policy is triggered and matches the specified filter.</p> <p>To add a new e-mail address to the list, click Add Email. Click the Enter Email Id field to enter the e-mail address. The e-mail address should be in the format user@example.com.</p> <p>To delete an e-mail address from the list, select the e-mail address and click Delete</p>	65535 characters	Blank
Send Traps to	Type the destinations where SNMP traps can be sent when an event occurs and matches the specified filter. See "Adding an SNMP Server" on page 106	Not applicable.	Not applicable.

Table 9: Notification Policy Table Command Button Descriptions

Element Name	Description	Privilege Required	Results
Edit filters and actions	Opens the Create Notification page, where you can edit the filters and actions of the selected notification policy.	Notifications	Opens the Create Notification page
Copy	Opens the Create Notification page, where you can create a copy of the selected notification policy.	Notifications	Opens the Create Notification page
Delete	Deletes the selected notification policy	Notifications	Removes the selected policies from the table

Table 9: Notification Policy Table Command Button Descriptions (*continued*)

Element Name	Description	Privilege Required	Results
Change Status	Opens the Change Notification Policy Status dialog box, where you can change the status of a notification policy from Enabled to Disabled or vice versa.	Notifications	Changes the status of the selected policies from Enabled to Disabled or vice versa

- Related Documentation**
- Notification Policies Overview on page 51
 - Enabling or Disabling a Notification Policy on page 57

Enabling or Disabling a Notification Policy

Notification policies specify the events for which Service Now sends notifications, and the actions that Service Now takes in response to these events. They define the events that trigger the notification, the filters that further specify the trigger events, and the actions that you want Service Now to take after the event is triggered.

To enable a notification policy:

1. From the Service Now task ribbon, select **Service Central** > **Notifications**.

The **Manage Notifications** page is displayed.

2. Select the notification policies whose status you want to change.
3. Select **Enable/Disable** from the Actions panel.

The **Change Reaction Policy Status** dialog box displays the name and status of the selected incident.

4. Click **Change Status** to confirm your action.

The status of the notification policy changes from **Enabled** to **Disabled** or vice versa.

- Related Documentation**
- Notification Policies Overview on page 51
 - Creating and Editing a Notification Policy on page 52

Deleting a Notification Policy

A notification policy specifies the events for which Service Now sends notifications, and the actions that Service Now takes in response to these events. It defines the events that trigger the notification, the filters that further specified the trigger events, and the actions that you want Service Now to take after the event is triggered.

To delete a notification policy:

1. From the Service Now task ribbon, select **Service Central > Notifications**.

The **Manage Notifications** page is displayed.

2. From the Notifications table, select the notification policy (or policies) that you want to delete.
3. Select **Delete** from the Actions panel.

The **Confirm Deletion of Notification Policies** dialog box displays the name of the notification policy and its owner.

4. Click **Delete**.

This action deletes the selected notification policies from the Service Now database and from the Notifications table.

**Related
Documentation**

- Notification Policies Overview on page 51
- Enabling or Disabling a Notification Policy on page 57

PART 4

Administration

- Administration Overview on page 59
- Organizations on page 63
- Device Groups on page 73
- Devices on page 77
- Event Profiles and Script Bundles on page 87
- Global Settings on page 103

Administration Overview

You can use Service Now to monitor and manage device data with the help of AI-Scripts that are installed on a device. When AI-Scripts are installed on a device, the device is AIS-enabled. It can then automatically detect and report incidents and informational JMBs (iJMBs).

Devices with AI-Scripts installed periodically send device data in the form of Informational Juniper Message Bundles (iJMBs) to Service Now . Users can view this information. Using Service Now you can add and manage devices, upload AI-Script bundles, and install the AI-Scripts on the devices. You can add devices that are part of the Junos Space platform to Service Now and group them under organizations.

An organization is defined by a unique site id that is a unique identifier of a customer record in Juniper Networks CRM systems. After creating an organization, you can test its connectivity with JSS and even run it in test mode. Juniper Support Systems (JSS) provides support for the incidents and iJMBs that you submit depending on your service contract level. J-Care Efficiency, Continuity, or Agility levels of service are required to use Service Now.

If you are a Juniper Networks partner or a direct customer with multiple distinct networks, you can use multiple Service Now organizations to keep customers or networks separate. Service Now organizations are defined by the site ID (used when opening support cases) under devices and users. Also, by associating an organization with one or more device groups, you can maintain groups of devices with similar attributes and control a user's access to devices. Device groups also help you automatically install AI-Scripts on many devices at one time.

Some administration tasks, such as adding connected members and viewing messages assigned to them, are enabled only when Service Now partner proxy mode is activated. For more information on Service Now modes, see "Service Now Modes" on page 9.

The Service Now sidebar includes a Getting Started section that guides the administrator through the initial setup required to get the application up and running. This section lists four required and two optional tasks. Clicking the task links displays the respective pages in the Inventory panel where these tasks can be performed.

The required tasks are:

1. Reviewing global settings.
2. Creating an organization.
3. Adding devices to Junos Space.
4. Creating a device group.
5. Installing AI-Scripts on devices.

The optional task is adding a new script bundle.

The Administration page graphically displays information about devices with respect to the device group they belong to, whether these devices are sending device snapshots periodically, and also the devices that have never sent device snapshots to Service Now. Using the Administration tab, you can perform the following tasks:

- Add devices to Service Now from the Junos Space platform.
- Add or delete a script bundle.
- Add and delete devices and device groups.
- Install or uninstall AI-Scripts on devices.
- Associate devices with device groups.
- Add, modify, or delete an organization.
- Add connected members and view messages assigned to them (enabled if you are a Service Now partner).
- Run organizations in test mode and test organization connectivity to JSS.
- Export device data in CSV and Excel formats.
- Configure the global settings (SNMP server and proxy server settings).

For more information, see the Junos Space documentation on the Juniper Networks technical documentation page.

**Related
Documentation**

- Service Now MIBs
- Service Now Overview on page 3
- Service Now Modes on page 9
- Service Now Devices Overview on page 77
- Device Groups Overview on page 73
- Script Bundles Overview on page 98

- Organizations Overview on page 63
- Configuring Global Settings on page 103

CHAPTER 12

Organizations

- Organizations Overview on page 63
- Adding an Organization on page 65
- Adding a Connected Member on page 67
- Modifying Organization Parameters on page 68
- Deleting an Organization on page 69
- Test the Connection to JSS on page 70
- Viewing Messages Assigned to a Connected Member on page 70
- Running an Organization in Test Mode on page 71

Organizations Overview

An organization in Service Now represents a unique Clarify site ID in Juniper Support Systems (JSS). Clarify Site IDs are used by JSS to identify customers when providing technical support. You can use multiple organizations defined in Service Now to manage multiple sites (each with its own Clarify site ID) with just one Service Now installation. This is done by dividing the network into multiple logical customer sites. To communicate with JSS, a Service Now organization requires a site ID, login name, and password. The login name must be a contact associated with the site ID.

Device groups are used to group devices within an organization. By associating an organization with one or more device groups, you can maintain groups of devices with similar attributes or uses. Using device groups, you can control the access that users have over devices. See “Device Groups Overview” on page 73.

For more information about creating device groups, see “Creating a Device Group” on page 73.

While you configure organizations to run Service Now in a preproduction environment, you can avoid the processing of production incident cases by running an organization in test mode. In this mode, the synopsis of the incident is appended with [Test] and JTAC recognizes the case as a test case and does not process it.

Service Now organizations are displayed on the **Manage Organizations** page. You can choose to display the organizations either as a table arranged according to name, site ID, submit cases as, username, and connection status, or as icons, as shown in Figure 8 on page 64.

Figure 8: Manage Organizations Page

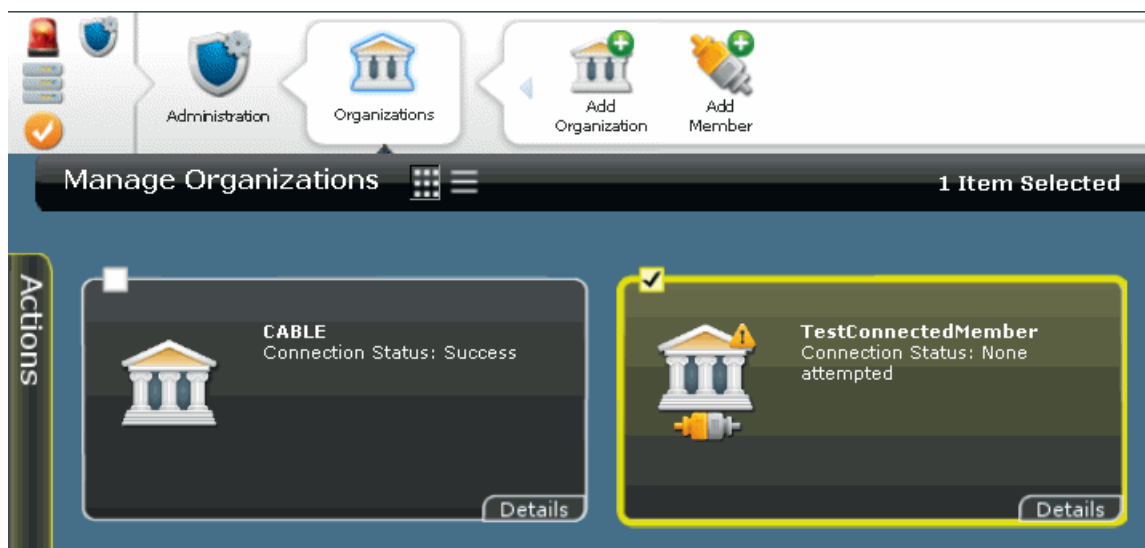


Table 10 on page 64 describes the fields displayed in the tabular view of the **Manage Organizations** page and in the **Organizations Details** dialog box.

Table 10: Organization Column Descriptions

Column Name	Description
Name	Name of the organization
Site ID	Identifier for the Customer Site in the JTAC Clarify system
Submit Cases As	Status of the case that is sent to JSS. It is a real case or a test case that is sent in a production environment. The synopsis of a test case sent to JSS is appended with [Test Mode].
User Name	Name used to identify the user for communications with the JTAC Clarify system, such as creating cases, and checking for updates to existing cases
Connection Status	Status of the connection between the organizations and JSS
JMB Filter Level	Amount of device configuration information in a JMB that can be shared with JSS

From the Organizations page, you can:

- Add an organization
- Modify organization parameters
- Run an organization in test mode
- Test connectivity to JSS
- Delete an organization

- Related Documentation**
- Adding an Organization on page 65
 - Modifying Organization Parameters on page 68
 - Running an Organization in Test Mode on page 71

Adding an Organization

An organization in Service Now represents a unique Clarify site ID in Juniper Support Systems (JSS). Clarify Site IDs identify customers when JSS provides technical support. You can use multiple organizations defined in Service Now to manage multiple sites (each with its own Clarify site ID) with only one Service Now installation. This is done by dividing the network into multiple logical customer sites. To communicate with JSS, a Service Now organization requires a site ID, login name, and password. While creating an organization you can specify the amount of device configuration information in JMBs that you want to share with JSS, for devices associated with that organization.



NOTE: In End Customer mode, you can add only one organization.

To add a Service Now organization:

1. From the Service Now task ribbon, select **Administration > Organizations > Add Organization**.

The **Add Organization** dialog box is displayed.

2. Enter the organization parameters in the provided fields.
For a detailed description of these fields, see Table 11 on page 66.
3. Click **Submit**.

This action verifies and saves the organization parameters and returns to the **Manage Organization** page.

Table 11 on page 66 defines the **Add Organization** dialog box fields.

Table 11: Organization Credentials Page Field Descriptions

Name	Description	Privileges	Range/Length	Default
Name	Name of the organization	Service Now administrator privileges	64 characters	Blank
Site ID	Identifier for the Customer Site in the JTAC Clarify system	Service Now administrator privileges	80 characters	Blank
Submit cases as	Status of the case that is sent to JSS. It is a real case or a test case that is sent in a production environment. The synopsis of a test case sent to JSS is appended with [Test Mode].	Service Now administrator privileges	The values are: <ul style="list-style-type: none"> Real cases Test cases 	Disabled
User Name	Name used to identify the user for communications with the JTAC Clarify system, such as creating cases, and checking for updates to existing cases	Service Now administrator privileges	32 characters	Blank
User Password	Password used to login, for the account with the user name you specify	Service Now administrator privileges	32 characters	Blank
Confirm User Password	Password for confirmation must match the value in User Password field	Service Now administrator privileges	32 characters	Blank
JMB Filter Level	Amount of device configuration information in JMBs to be shared with JSS: <ul style="list-style-type: none"> Do not send—Sends no configuration information Send all information except configuration—Sends all device information except the configuration Send all information with IP Addresses overwritten—Sends all device information, except IP addresses Send all information—Sends all device information. Only send list of features used—Sends only the device configuration information 	Service Now administrator privileges	Not applicable.	Do not send

Related Documentation

- Organizations Overview on page 63
- Running an Organization in Test Mode on page 71

Adding a Connected Member

After you configure Service Now to run in partner proxy mode, you can add multiple end customers and manage end customer Service Now applications over a secure https connection. The partner proxy can communicate with the end customer only after the Service Now application of an end customer is activated. For more information about partner proxy and end customer modes, see “Service Now Modes” on page 9.



NOTE: You can add a connected member only after you create a valid organization.

To add a connected member to Service Now:

1. From the Service Now task ribbon select, **Administration > Organization > Add Connected Member**.

The **Add Member** dialog box is displayed as shown in Figure 9 on page 67.

Figure 9: Add Member Dialog Box

The screenshot shows the 'Add Member' dialog box with the following fields and controls:

- Name:** Text input field
- User Name:** Text input field
- User Password:** Text input field
- Confirm User Password:** Text input field
- JMB Filter Level:** Dropdown menu with 'Do not send' selected
- Organization:** Dropdown menu with 'Please select ...' selected
- Submit:** Blue button
- Cancel:** Red button

2. Enter a name for the connected member.
The name must begin with an alphanumeric character (a-z, 0-9), and can contain underscores (_), spaces, and hyphens (-).
3. Enter a username for the connected member.
The username must be in the format user@example.com.
4. Enter the password that can be used to log in with the user name you have entered.
5. Enter the same password again to confirm.
6. Select one of the following values to specify the amount of device configuration information in a JMB that can be shared with JSS:

- Do not send—Sends no configuration information
 - Send all information except configuration—Sends all device information except the configuration
 - Send all information with IP Addresses overwritten—Sends all device information, except IP addresses
 - Send all information—Sends all device information
 - Only send list of features used—Sends only the device configuration information
7. Select the organization with which the end customer can be associated. Ensure that you select an organization that has partner proxy credentials.
 8. Click **Submit**.

The connected member is created and displayed on the **Manage Organizations** page.

**Related
Documentation**

- Adding an Organization on page 65
- Organizations Overview on page 63

Modifying Organization Parameters

Using Service Now, you can modify the parameters of an organization.



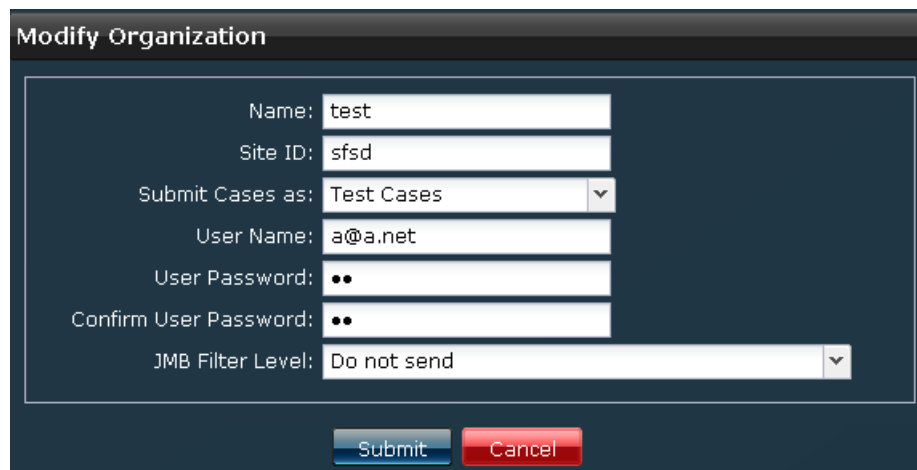
NOTE: When you modify the parameters of a connected member, you cannot edit the name of the connected member and the organization associated with it. For more information about connected members see “Service Now Modes” on page 9.

To modify the parameters of an organization:

1. From the Service Now task ribbon, select **Administration > Organizations**.
The **Manage Organizations** page is displayed.
2. Select the organization whose parameters you want to modify.
3. Select **Modify Organization** from the Actions panel.

The **Organizations** dialog box displays the name, site ID, submit cases as, user name, and password, and the JMB filter level of the selected organization.

Figure 10: Modify Organization Dialog Box



4. Make your changes to these parameters.
5. Click **Submit**.

The changes are saved in the Service Now database. To view these changes, view the details of the organization on the **Manage Organizations** page.

Related Documentation

- Organizations Overview on page 63
- Running an Organization in Test Mode on page 71

Deleting an Organization

You can use the Service Now **Manage Organizations** page to delete organizations. To do this, you need Service Now administrator privileges.

You cannot delete an organization without deleting its associated connected members.

To delete an organization:

1. From the Service Now task ribbon, select **Administration > Organizations**.
The **Manage Organizations** page is displayed.
2. Select the organization that you want to delete.
3. Select **Delete Organization** from the Actions panel.

The **Delete Organizations** dialog box prompts you to confirm the deletion.

4. Click **Delete**.

The selected organization is deleted from the Service Now database and no longer appears on the **Manage Organizations** page.



NOTE: Deleting an organization also removes associated device groups.

**Related
Documentation**

- Organizations Overview on page 63
- Running an Organization in Test Mode on page 71

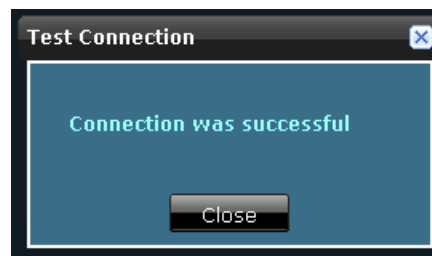
Test the Connection to JSS

From the **Manage Organizations** page, you can test an organization's connectivity with Juniper Support Systems (JSS). This test can be performed with every organization in the table.

To test an organization's connectivity with JSS:

1. From the Service Now task ribbon, select **Administration > Organizations**.
The **Manage Organizations** page is displayed.
2. Select the organization whose connection to JSS you want to test.
3. Select **Check Status** from the Actions panel.

The **Test Connection** dialog box displays the result of the test connection to JSS, as a success or a failure.



In case of a failure, a description is displayed, stating the reason for the failure in connection.

4. Click **Close** to return to the **Manage Organizations** page.

**Related
Documentation**

- Organizations Overview on page 63
- Running an Organization in Test Mode on page 71

Viewing Messages Assigned to a Connected Member

Using Service Now, you can view the list of messages that are assigned to a connected member. This action is available only when Service Now operates in partner proxy mode and when you select a connected member on the **Manage Organizations** page.

To view the messages assigned to a connected member:

1. From the Service Now task ribbon, select **Administration > Organizations**.

The **Manage Organizations** page displays the list of organizations and connected members.

2. Select the connected member whose list of assigned messages you want to view.
3. Right-click your selection or use the **Actions** panel and select **View Messages**.

As shown in Figure 11 on page 71, the **Messages assigned to Connected Member** page displays the list of messages assigned to the selected connected member.

Figure 11: Messages Assigned to Connected Member page

Messages assigned to Connected Member		
Return to Organization		
Title ▲	Status	Sent
abc	Delivered	2010/05/07 01:36
final1	Delivered	2010/05/07 01:36

4. To view the details of the messages, click the title of the message.

The **Message Details** dialog box displays information such as the organization that the message is sent to, site ID, title, issue date, summary, instructions, keywords, relevance, owner, and the users that the message was flagged to.

5. Click **Return to Organization** to return to the **Manage Organizations** page.

Related Documentation

- Assigning a Message to a Connected Member on page 43
- Messages Overview on page 41

Running an Organization in Test Mode

While configuring an organization, you can enable the test mode to submit cases as test cases to avoid the processing of production incident cases. In this mode, the synopsis of the incident that is being submitted to JTAC is appended with [Test].

To run an organization in test mode:

1. From the Service Now task ribbon, select **Administration > Organizations**.

The **Manage Organizations** page is displayed. If the table is empty, you need to add organizations.

2. Select the organizations that you want to place in test mode.
3. Select **Modify Organization** from the Actions list.

The **Organization** dialog box displays the parameters of the selected organization.

4. From the **Submit Cases as** list, select **Test Cases**.

5. Click **Submit**.

This action ensures that incidents that are submitted to JSS are considered as test cases.

- Related Documentation**
- Organizations Overview on page 63
 - Modifying Organization Parameters on page 68

CHAPTER 13

Device Groups

- Device Groups Overview on page 73
- Creating a Device Group on page 73
- Modifying Device Groups on page 74
- Deleting Device Groups on page 75

Device Groups Overview

You use device groups to group devices within an organization. By associating an organization with one or more device groups, you can maintain groups of devices with similar attributes or uses. You can associate one or more devices with every device group

Only users with Service Now administrator privileges can configure device groups.

From the **Manage Device Groups** page in Service Now, you can perform the following tasks:

- Creating and Adding Devices to a Device Group
- Modifying Device Groups
- Deleting Device Groups

Related Documentation

- Creating a Device Group on page 73
- Modifying Device Groups on page 74
- Deleting Device Groups on page 75

Creating a Device Group

You use device groups to group devices within an organization. Only users with Service Now administrator privileges can create device groups and add devices to them.

To create a device group:

1. From the Service Now task ribbon, select **Administration > Device Groups > Create Device Group**.

The **Administration: Create Device Group** page is displayed.

2. Enter a name for the device group within the **Name** field.
The name must begin with a letter and can have only alphanumeric characters (a-z, 0-9), underscores(_), and hyphens (-).
3. From the **Organizations** list, select an organization for this device group.
If you want to add a new organization, click **New Organization**. See “Adding an Organization” on page 65.
4. Select the devices that you want to add to this device group.
5. Click **Finish**.

The selected devices are added to the device group. To verify that the devices have been added, you can view the details of the device group on the **Manage Device Groups** page.

- Related Documentation**
- Device Groups Overview on page 73
 - Modifying Device Groups on page 74

Modifying Device Groups

You can modify the parameters of a device group in Service Now.

To modify a device group:

1. From the Service Now task ribbon, select **Administration > Device Groups**.
The **Manage Device Group** page lists the existing device groups.
2. Select the device group whose parameters you want to modify.

3. Select **Modify Device Group** from the Actions panel.

The **Modify Device Group** dialog box displays the parameters of the selected device group.

4. Make your modifications.
Use the **Device Groups** navigation panel on the right to add or delete devices from the selected device group.

5. Click **Finish**.

The changes are submitted and new values are replaced in the Service Now database. The **Manage Device Group** page is displayed.

**Related
Documentation**

- Device Groups Overview on page 73
- Deleting Device Groups on page 75
- Creating a Device Group on page 73

Deleting Device Groups

If you have Service Now administrator privileges, you can delete device groups.

To delete a device group:

1. From the Service Now task ribbon, select **Administration > Device Groups**.

The **Manage Device Group** page lists the existing device groups.

2. Select the device group that you want to delete.
3. Select **Delete Device Group** from the Actions panel.

The **Delete Device Group** dialog box prompts you to confirm the deletion.

4. Click **Delete**.

The selected device group is deleted from the Service Now database and no longer appears on the **Manage Device Group** page.

**Related
Documentation**

- Device Groups Overview on page 73
- Modifying Device Groups on page 74

CHAPTER 14

Devices

- Service Now Devices Overview on page 77
- Adding Devices from the Platform on page 80
- Installing an Event Profile on Devices Using Service Now on page 80
- Installing AI-Scripts Manually on Devices on page 82
- Uninstalling Event Profiles from Devices on page 84
- Exporting Device Data in CSV and Excel Format on page 84
- Deleting a Device on page 85
- Associating Devices to a Device Group on page 85

Service Now Devices Overview

You can use Service Now to group network elements and manage multiple devices in a single entity called a device group. Service Now lists the devices that are already a part of the Junos Space platform and that you can import into Service Now. These devices periodically send device information to Service Now for monitoring purposes. Service Now detects and displays devices that do not send device information (device snapshots) for more than 2 weeks.

After you add devices and create device groups, you can perform various operations on them, such as installing and uninstalling AI-Scripts individually on every device or on all the devices in a device group at once, and also deleting them from the Service Now database. Service Now devices are displayed on the **Service Now Devices** page. You can choose to display the devices either as a table arranged according to organization, device group, hostname, serial number, platform, version, and script bundle, or as icons, as shown in Figure 12 on page 78. Table 12 on page 78 describes the columns on the **Service Now Devices** page and the **Device Detail** dialog box.

Figure 12: Service Now Devices Page

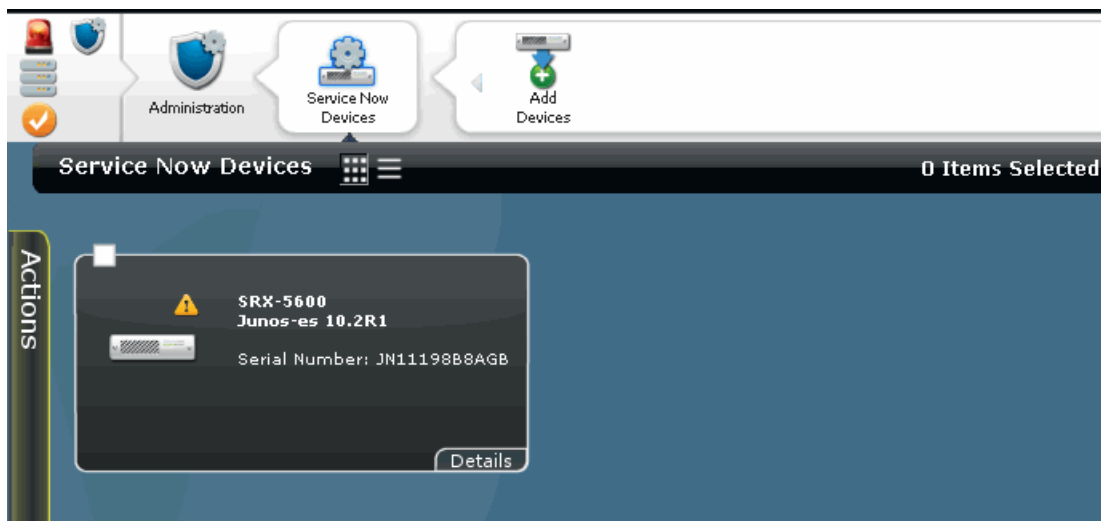


Table 12 on page 78 describes the fields displayed in the tabular view of the **Service Now Devices** page and in the **Device Details** dialog box.

Table 12: Service Now Devices Column Descriptions

Field Name	Description
HostName	Unique name by which the device is known on a network
Serial Number	Serial number of device.
Platform	Type of device (routing platform).
OS Version	Version of the Junos operating system that is running on the device
Organization	Name of the organization to which this device belongs
Device Group	Name of the device group to which this device belongs
Script Bundle	Name and version of the script bundle installed on the device
Routing Engine	Type of routing engine. The values are: <ul style="list-style-type: none"> • Single RE • Dual RE
AI-Script Installation Status	Status of AI-Script installation on the device. The values are: <ul style="list-style-type: none"> • Success • Failed • Master RE Failed • Backup RE Failed • Successfully installed in Master RE. Backup RE is inactive.

Table 12: Service Now Devices Column Descriptions (*continued*)

Field Name	Description
Connection Status	Status of connection from the device to Service Now
Device Snapshot Status	Status of iJMB upload

From the Service Now Devices page you can perform the following tasks:

- Add devices from the platform
- Install AI-Script on devices
- Uninstall AI-Script from devices
- Export device data into CSV and Excel format
- Modify device parameters
- Delete devices
- Associate devices with a device group

**Related
Documentation**

- Adding Devices from the Platform on page 80
- Installing an Event Profile on Devices Using Service Now on page 80
- Uninstalling Event Profiles from Devices on page 84
- Exporting Device Data in CSV and Excel Format
- Modifying Device Groups on page 74
- Deleting a Device on page 85
- Associating Devices to a Device Group on page 85

Adding Devices from the Platform

You can add devices that are a part of the Junos Space platform to the Service Now application. While you add these devices, you can assign them to a device group and also install AI-Scripts on them.



NOTE: Devices that are discovered and added to the Junos Space platform are automatically added to the Service Now application. However, if Service Now is in demo mode, only the first five devices are added.

To add devices from the Junos Space platform to Service Now:

1. From the Service Now task ribbon, select **Administration > Service Now Devices > Add Devices**.

The **Select Devices to Add to Service Now and Click Next or Finish** page displays the devices that have not been added to Service Now.

Select Devices to Add to Service Now and Click Next or Finish					Add Devices	
<input type="checkbox"/>	Host Name	Network Name	SSH User Name	SSH Password	Device Status	
<input type="checkbox"/>	puppy	10.204.92.75	regress	*****	Imported	Add Devices
<input type="checkbox"/>	junoscopea	10.204.92.63	regress	*****	Imported	Install AI Scripts

2. Select the devices that you want to add.
3. (Optional) To install script bundles on the selected devices, click **Install AI Scripts** or click **Next** and select the **Install AI Scripts on new Devices** check box.

For more information about installing AI-Scripts on devices, see “Installing an Event Profile on Devices Using Service Now” on page 80. If you are unable to install AI-Scripts, ensure that the device has proper login credentials and belongs to a device group.

4. Click **Finish**.

The devices are added to Service Now and displayed on the **Service Now Devices** page. The device **Status** column displays **Imported**.

Related Documentation

- Service Now Devices Overview on page 77

Installing an Event Profile on Devices Using Service Now

An event profile is a set of event scripts that are selected from an AI-Script bundle. When you install an event profile on Juniper Networks devices, the event scripts are installed on the devices and provide the information needed to automatically detect and report problem (incident) and information events, thus ensuring maximum network uptime. Service Now uses Device Management Interface (DMI) to install and uninstall AI-Scripts on devices. DMI is an extension to the NETCONF network management protocol.

When you install event profiles on individual systems (chassis) with dual Routing Engines, Service Now installs the event profiles on both primary and backup Routing Engines.



NOTE: Read the KB article, <http://kb.juniper.net/KB19155>, before installing AI-Scripts on devices.



NOTE: While operating in partner proxy mode, you cannot install event profiles on a connected member's device.

To install an event profile on devices:

1. From the Service Now task ribbon, select **Administration > Service Now Devices**.

The **Service Now Devices** page is displayed.

2. Select the device on which you want to install the event profile.



NOTE: You can install event profiles on only those devices for which you can specify correct login credentials and that belong to a device group.

3. Select **Install Event Profile** from the **Actions** panel.

The **Install Event Profile** dialog box is displayed as shown in Figure 13 on page 81.

Figure 13: Install Event Profile Dialog Box

4. Select an event profile from the **Use Profile** list, which displays the event profiles that you upload into Service Now.
5. (Optional) If you do not want to save a copy of the event profile after it is installed on the device, select the **Never store Script Bundle files on device (if selected roll-back option will not be available)** check box.
6. (Optional) If you want to remove the script bundle from the device, after it is installed, select the **Remove Script Bundle files after successful install** check box.
7. (Optional) If you want to schedule a time for installation, select the **Schedule at a later time** check box, and specify the **Date and time** for the installation.

The installation process begins automatically at the time you specify.

8. Click **Submit**.

The event profile installation task is scheduled and the **Job Information** dialog box displays the job ID.

To view the status of this task, click the job ID link. The **Manage Jobs** page displays the status of the job. The **Device Details** dialog box also displays the status of AI-Script installation for the selected devices.

If you have installed the event profile on a dual Routing Engine, the results (displayed on the **Manage Jobs** page) shows the status for both primary Routing Engine and the backup Routing Engine. The status of the job says **Failed** if the installation fails on either of the Routing Engines.



9. Click **OK**.

The **View Event Profiles** page is displayed.

**Related
Documentation**

- Event Profiles Overview on page 87
- Script Bundles Overview on page 98
- Installing AI-Scripts Manually on Devices on page 82
- Adding a Script Bundle to Service Now on page 99

Installing AI-Scripts Manually on Devices

AI-Scripts can be installed on Junos OS devices manually using CLI mode. Service Now also uses the loopback interface on Junos OS devices for collecting the Juniper Message Bundle (JMB) when an event occurs.



NOTE: If you do not want to use loopback address, you can use the management IP address for collecting JMBs in the archive-sites [/var/tmp].

To enable communication using the loopback address, add the following firewall rules:

```
set firewall family inet filter scp-block term ais-scp from source-address
127.0.0.1/32
set firewall family inet filter scp-block term ais-scp from destination-address
127.0.0.1/32
set firewall family inet filter scp-block term ais-scp from protocol tcp
```

```

set firewall family inet filter scp-block term ais-scp from port 22
set firewall family inet filter scp-block term ais-scp then accept
Rouer001# show firewall family inet filter scp-block term ais-scp
from { source-address {
127.0.0.1/32;
}
destination-address {
127.0.0.1/32;
} protocol tcp;
port 22;
}
then accept;

```



NOTE: For manual installation of AI-Scripts on a device, you require the login credentials used to discover devices in Junos Space.

To install AI-Scripts manually:

1. Copy the AI-Script bundle (example: jais-2.1R2.0-signed.tgz) to the Junos OS device using SCP or FTP.
2. From configuration mode, execute the following commands:
set groups juniper-ais system scripts commit allow-transients
set groups juniper-ais system scripts commit file jais-activate-scripts.slax optional
set groups juniper-ais interfaces lo0 unit 0 family inet address 127.0.0.1/32
set groups juniper-ais event-options destinations juniper-aim archive-sites
"scp://<user>@127.0.0.1://var/tmp" password <password for user>
3. Install the AI-Script bundle in CLI mode using the command
request system scripts add <full-path>/jais-2.1R2.0-signed.tgz

The AI-Script is installed on the device.

Related Documentation

- Installing an Event Profile on Devices Using Service Now on page 80
- Adding a Script Bundle to Service Now on page 99

Uninstalling Event Profiles from Devices

You can use Service Now to uninstall event profiles from devices. You cannot uninstall event profiles from devices that do not have proper login credentials. Service Now uses Device Management Interface (DMI) to install and uninstall event profiles on devices. DMI is an extension to the NETCONF network management protocol.



NOTE: While operating in Partner Proxy mode, you cannot uninstall event profiles from a connected member's device.

To uninstall event profiles from devices:

1. From the Service Now task ribbon, select **Administration > Service Now Devices**.
The **Service Now Devices** page is displayed.
2. Select the devices from which you want to uninstall event profiles.
3. From the Actions drawer, or the right click context menu, select **Uninstall Event Profile**.
You are prompted to confirm the deletion.
4. Click **Submit**.

This event profiles are uninstalled from the selected devices.

Related Documentation

- Script Bundles Overview on page 98
- Installing an Event Profile on Devices Using Service Now on page 80

Exporting Device Data in CSV and Excel Format

You can export Service Now device data in CSV and Excel file formats. A CSV file is a plain text file that stores each data record separated by a comma. The XML file contains the hardware components installed in the selected device.

To export the device data in CSV and Excel format:

1. From the Service Now task ribbon, select **Administration > Service Now Devices**.
The **Service Now Devices** page is displayed.
2. Select the device whose data you want to export.
3. Select **Export Devices** from the Actions panel.
The **Export Devices** dialog box displays the links to the CSV and Excel files.
4. Select the links to save the files in CSV and Excel file formats.

Related Documentation

- Service Now Devices Overview on page 77
- Deleting a Device on page 85

Deleting a Device

When you delete a device, the device is deleted from Service Now, but it is not deleted from the Junos Space Platform. The incidents and JMBs related to the device are also deleted.

To delete a device from Service Now:

1. From the Service Now task ribbon, select **Administration > Service Now Devices**.

The **Service Now Devices** page lists the Service Now devices.

2. Select the device that you want to delete.
3. Select **Delete** from the Actions panel.

The **Delete** dialog box prompts you to confirm the deletion.

4. Click **Delete** again.

The selected device is deleted from the Service Now database and is no longer displayed on the **Service Now Devices** page.

Related Documentation

- Service Now Devices Overview on page 77
- Modifying Device Groups on page 74

Associating Devices to a Device Group

Service Now associate devices with device groups.

To associate devices with device group:

1. From the Service Now task ribbon, select **Administration > Service Now Devices**.

The **Service Now Devices** page lists the Service Now devices.

2. Select the device that you want to associate with a device group.
3. Select **Associate Device Groups** from the Actions panel.

The **Associate Device Groups** dialog box is displayed.

4. From the **Device Group** list, select the device group that you want to associate with the selected device.
5. Click **Submit**.

The device are associated with the selected device group. You can verify the changes on the **Service Now Devices** page, in the Device Group column.

Related Documentation

- Service Now Devices Overview on page 77
- Modifying Device Groups on page 74

CHAPTER 15

Event Profiles and Script Bundles

- Event Profiles Overview on page 87
- Adding an Event Profile on page 89
- Cloning an Event Profile on page 91
- Deleting Event Profiles on page 92
- Viewing an Event Profile on page 93
- Pushing an Event Profile to Devices on page 94
- Displaying Devices Associated with an Event Profile on page 95
- Setting an Event Profile as Default on page 96
- Exporting Events Data in Excel Format on page 97
- Script Bundles Overview on page 98
- Adding a Script Bundle to Service Now on page 99
- Setting a Script Bundle as Default on page 100
- Deleting a Script Bundle from Service Now on page 101

Event Profiles Overview

An event profile is a set of event scripts selected from an AI-Script bundle. Using event profiles, you can specify the event scripts that you want to install on Service Now devices.

To create an event profile, you need an AI-Script bundle from which you can select the event scripts that you want to associate with the event profile. The set of event scripts can be updated using the latest AI-Script bundles.

When you install Service Now, the latest AI-Script bundle is preloaded and displayed on the Manage Script Bundles page. You can also download other AI-Scripts bundles from the Juniper Networks software download site and upload them to Service Now (see “Adding a Script Bundle to Service Now” on page 99).

In Service Now, there is always an event profile and an AI-Script bundle that is set as the default. The default event profile is always associated with an AI-Script bundle. For new Service Now installs or upgrades the default event profile is associated with the preloaded AI-Script bundle (i.e. the AI-Script bundle that is available with Service Now). After installing or upgrading Service Now, you can add additional AI-Script bundles and set any AI-Script bundle and event profile as the default. The default script bundle is

automatically selected while creating a new event profile and the default event profile is automatically selected while installing an event profile on devices.

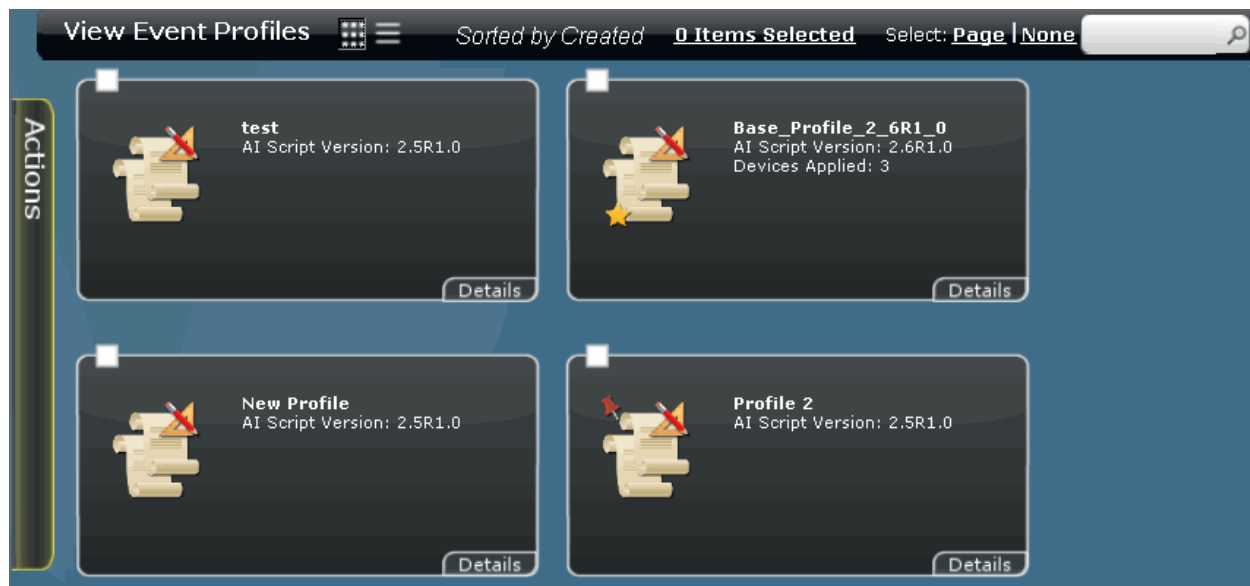


NOTE: Read the KB article, <http://kb.juniper.net/KB19155>, before installing AI-Scripts on devices.

Service Now allows you to clone an existing event profile by modifying its name, description, script bundle, set of included event scripts, and event script priorities. Cloning an event profile allows you to make changes without losing the original event profile. After you make your modifications, you can save the cloned event profile and apply it over the original event profile for devices where the original event profile was installed. You can also install the new event profile on any other devices. The priority values of event scripts determine the priority shown in the JMBs generated for a Service Now event. After you install event profiles on devices, you can filter and display only the devices that are associated with a specific event profile. Service Now also enables you to export events data that is specific to an event profile in Excel format and delete event profiles that are not associated with devices.

In Service Now, event profiles are displayed on the **View Event Profiles** page (Figure 14 on page 88). The tabular view of the **View Event Profiles** page displays information about the event profile including the total number of incidents generated per event in the event profile, the total number of active events, the total number of inactive events, the number of devices on which the event profile is installed, most active events, least active events, and inactive events. The default event profile and the event profiles that are installed on the devices are represented by two unique icons. For example, as shown in Figure 14 on page 88, **Profile 2** is the default event profile, and **Base_Profile_2.6R1_0** is an event profile that is installed on the devices.

Figure 14: View Event Profiles Page



Using the **Event Profiles** workspace, you can perform the following tasks:

- Adding an Event Profile on page 89
- Pushing an Event Profile to Devices on page 94
- Displaying Devices Associated with an Event Profile on page 95
- Setting an Event Profile as Default on page 96
- Exporting Events Data in Excel Format on page 97
- Viewing an Event Profile on page 93
- Cloning an Event Profile on page 91
- Deleting Event Profiles on page 92

**Related
Documentation**

- Installing an Event Profile on Devices Using Service Now on page 80

Adding an Event Profile

An event profile is a set of scripts that are selected from an AI-Script bundle. Using event profiles, you can specify the event scripts you want to install on the devices. To add an event profile, you can use the default AI-Script bundle that is available when you install Service Now, or upload a new AI-Script bundle (see “Adding a Script Bundle to Service Now” on page 99).

After you add a script bundle to Service Now, to be able to install the script bundle on the devices, you must create an event profile using this script bundle.

To add an event profile:

1. From the Service Now task ribbon, select **Administration > Event Profiles > Add Event Profile**.

The **Add Event Profile** page is displayed. For a description about the fields displayed on this page, see Table 13 on page 90.

2. Enter an event profile name.
3. (Optional) Enter a description about the event profile.
4. Select an AI-Script bundle from the **AI-Script Bundle** drop-down list.

By default, the AI-Script bundle that is set as the default is automatically selected and you can modify this selection if required.

5. (Optional) To add a new script bundle, click **Add Script Bundle** (see “Adding a Script Bundle to Service Now” on page 99).
6. Select the event scripts that you want to install on the device. By default, only the event scripts that are enabled (on the device) are selected.
7. Click **Submit**.

An event profile is created with your specifications. To verify, you can view the details of the event profile displayed on the **Manage Event Profiles** page.

Table 13: Add Event Profile Page Field Descriptions

Field	Description
Profile Name	Name of the event profile that you specify
Description	Explanation that you specify about the event profile
AI-Script Bundle	List of AI-Script bundles that are available in Service Now. This consists of the default AI-Script bundle that is available with Service Now and the ones that you upload.
Event Scripts	List of event scripts that are available with the AI-Script bundle you select within the AI-Script Bundle field
Name	Name used to identify the event script.
Type	Type of event that triggers the event script: <ul style="list-style-type: none"> • Hardware failure • Software failure • Resource Exhaustion
Sub type	Detailed description about the type of event that triggers the event script. For example, file system error, communication error, socket failure, excessive memory utilization, database failure, session error, memory allocation error, initialization error, process error, and so on.
Description	Synopsis about the event script
Priority	Priority level of the event script. The values are: <ol style="list-style-type: none"> 1. Low 2. Medium 3. High 4. Severe
Occurrence (last 90)	Number of times the event occurred in the last 90 days
Occurrence (Total)	Total number of times the event occurred
Unique Devices	Number of times the event occurred on unique devices
Top Devices	Devices on which the event occurred maximum number of times

Related Documentation

- Pushing an Event Profile to Devices on page 94
- Displaying Devices Associated with an Event Profile on page 95
- Event Profiles Overview on page 87

Cloning an Event Profile

Service Now allows you to clone an existing event profile and modify its name, description, script bundle, set of included event scripts, and event script priorities to create another event profile. After you clone an event profile, you can redeploy the event profile or deploy the event profile on new devices. The priority values of event scripts determine the priority of the Juniper message bundles (JMBs) that the scripts generate. When you clone an event profile, the original parameters of the event profile are displayed, but the event profile name is appended with **Copy of**.

To clone an event profile:

1. From the Service Now task ribbon, select **Administration > Event Profiles**.
The **Manage Event Profiles** page is displayed.
2. Select the event profile that you want to clone.
3. Right-click your selection or use the **Actions** panel and select **Clone**.

As shown in Figure 15 on page 91, the attributes of the event profile (in the following example, test) that you selected are displayed in an editable format.

Figure 15: Clone Event Profile page

Profile Name:

Description:

Script Bundle:

Events:

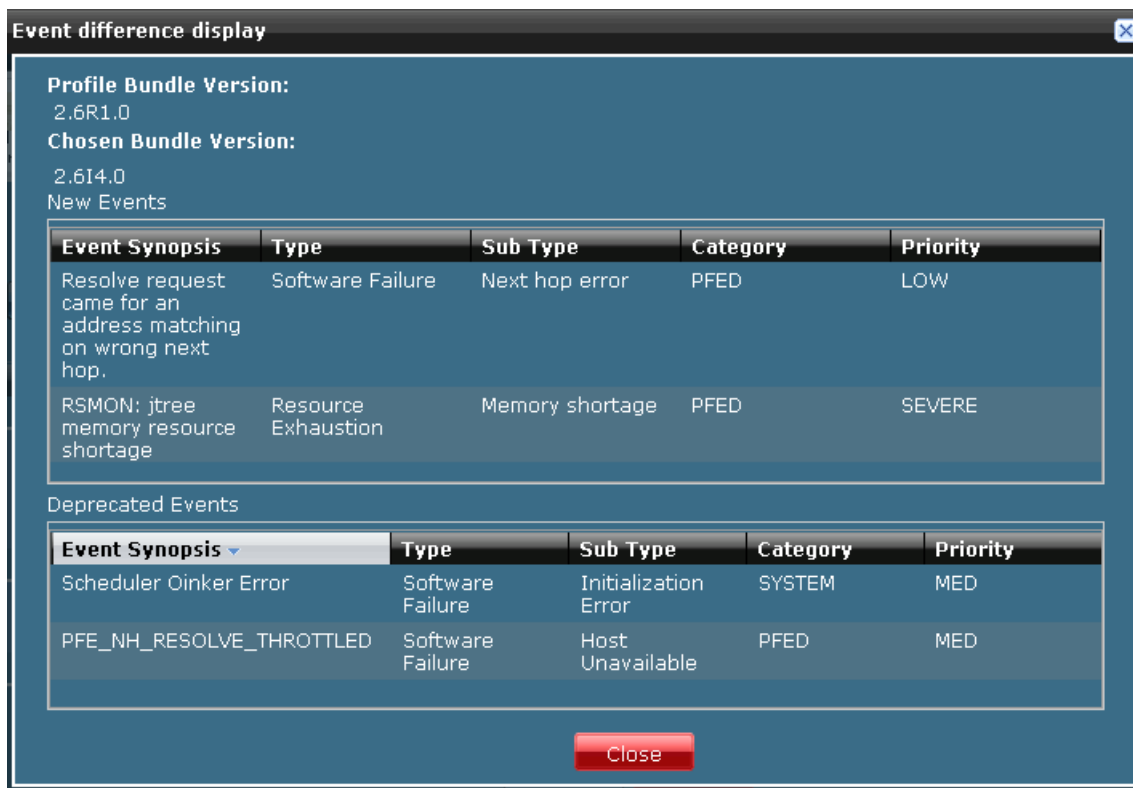
Event Synopsis	Type	Sub Type	Priority (editable)
Category: ACCT (1 Item)			
<input checked="" type="checkbox"/> ACCT_XFER_POPEN_FAIL	Software Failure	Communication Error	Medium
Category: ASP (2 Items)			
<input checked="" type="checkbox"/> ASP_IDS_INV_CLEAR_QUERY	Software Failure	Unexpected output	High
<input checked="" type="checkbox"/> ASP_IDS_INV_CLEAR_QUERY_VER	Software Failure	Unexpected output	High
Category: ASP_L2TP (1 Item)			
<input checked="" type="checkbox"/> ASP_L2TP_NO_MEM	Resource Exhaustion	Memory Consumption	Medium
Category: AUDITD (3 Items)			

Page 1 of 4 | Displaying 1 - 100 of 383

4. Make your modifications to the event profile name, description, script bundle, set of included event scripts, and event script priorities.

5. (Optional) While selecting a different script bundle, you can compare the event scripts of the original and new script bundles. To compare:
 - a. From the **Script Bundle** list, select the script bundle that you want to compare. The **Show Difference** button is displayed.
 - b. Click the **Show Difference** button.
As shown in Figure 16 on page 92, the **Event difference display** dialog box lists the new and deprecated events by comparing the two event profiles that you selected.

Figure 16: Event difference display dialog box



- c. Click **Close**.
6. Click **Submit**.
The event profile is created and displayed on the **Manage Event Profiles** page.

- Related Documentation**
- Pushing an Event Profile to Devices on page 94
 - Event Profiles Overview on page 87

Deleting Event Profiles

Using Service Now, you can delete multiple event profiles. You can delete an event profile only if it is not associated with a device.



NOTE: When you delete the default event profile, the latest created profile is automatically set as the default.

To delete event profiles:

1. From the Service Now task ribbon, select **Administration > Event Profiles**.
The **Manage Event Profiles** page is displayed.
2. Select the event profiles that you want to delete.
3. Right-click your selection or use the **Actions** panel, and select **Delete**.
The **Delete Event Profiles** dialog box displays the list of event profiles that you selected.
4. Click **Delete** to confirm.
The selected event profiles are deleted. To verify, you can check the list of event profiles displayed on the **Manage Event Profiles** page.

Related Documentation

- Displaying Devices Associated with an Event Profile on page 95
- Cloning an Event Profile on page 91
- Pushing an Event Profile to Devices on page 94

Viewing an Event Profile

Using Service Now, you can view an event profile's name, its description, the AI-Script bundle that it is associated with, and the event scripts that it consists of.

To view the event scripts that are part of an event profile:

1. From the Service Now task ribbon, select **Administration > Event Profiles**.
The **Manage Event Profiles** page is displayed.
2. Select the event profile whose details you want to view.
3. Right-click your selection or use the **Actions** panel, and select **View Events**.
The **Event Profiles** page displays the event profile's name, its description, the AI-Script bundle that it is associated with, and the event scripts that it consists of. The event script details includes the event script names, types, sub types, descriptions, priorities, occurrences in the last 90 days, the total number of occurrences, the number of unique devices, and the number of top devices.
4. Click **OK** to return to the **Manage Events** page.

Related Documentation

- Exporting Events Data in Excel Format on page 97
- Cloning an Event Profile on page 91
- Pushing an Event Profile to Devices on page 94

Pushing an Event Profile to Devices

An event profile is a set of event scripts that are selected from an AI-Script bundle. When you push an event profile onto Juniper Networks devices, these event scripts are installed on the devices. The event scripts provide the information needed to automatically detect and report problem (incident) and information events. Service Now uses Device Management Interface (DMI) to install and uninstall event profiles on devices. DMI is an extension to the NETCONF network management protocol.

When you install event profiles on individual systems (chassis) with dual Routing Engines, Service Now installs the event profiles on both the primary and backup Routing Engines.



NOTE: While operating in partner proxy mode, you cannot push event profiles to a connected member's device.

To install an event profile on devices:

1. From the Service Now task ribbon, select **Administration > Event Profiles**.

The **View Event Profiles** page is displayed.

2. Select the event profile that you want to push to devices.



NOTE: You can install event profiles only on devices for which you can specify correct login credentials and that belong to a device group.

3. Select **Push to devices** from the **Actions** panel.

The **Install Event Profile** dialog box is displayed (Figure 17 on page 94).

Figure 17: Install Event Profile Dialog Box

Install Event Profile

Profile Name: Base_Profile_2.5R1.0
Script Name: jais-2.5R1.0-signed.tgz

Select Devices to Install Profile

Organization	Device Group	Hostname	Serial Number
<input type="checkbox"/> UHH	test	10.204.92.69	
<input type="checkbox"/> UHH	test	10.204.92.23	

Page 1 of 1 | Displaying 1 - 2

☐ Never store Script Bundle files on device (if selected roll-back option will not be available)
☐ Remove Script Bundle files after successful install

☒ Schedule at a later time

Date and time: 01/04/11 11:04 AM IST

Submit Cancel

4. Select the devices on which you want to install the event profile.
5. (Optional) If you do not want to save a copy of the event profile after it is installed on the device, select the **Never store Script Bundle files on device (if selected roll-back option will not be available)** check box.
6. (Optional) If you want to remove the script bundle from the device, after it is installed, select the **Remove Script Bundle files after successful install** check box.
7. (Optional) If you want to schedule a time for installation, select the **Schedule at a later time** check box, and specify the **Date and time** for the installation. The installation process begins automatically at the time you specify.
8. Click **Submit**.

The event profile installation task is scheduled and the **Job Information** dialog box displays the job ID.

To view the status of this task, click the job ID link. The **Manage Jobs** page displays the status of the job. The **Device Details** dialog box also displays the status of AI-Script installation for the selected devices.

If you have installed the event profile on a dual Routing Engine, the results (displayed on the **Manage Jobs** page) shows the status for both the primary Routing Engine and the backup Routing Engine. The status of the job says **Failed** if the installation fails on either of the Routing Engines.

9. Click **OK**.

The **View Event Profiles** page is displayed.

Related Documentation

- Displaying Devices Associated with an Event Profile on page 95
- Cloning an Event Profile on page 91

Displaying Devices Associated with an Event Profile

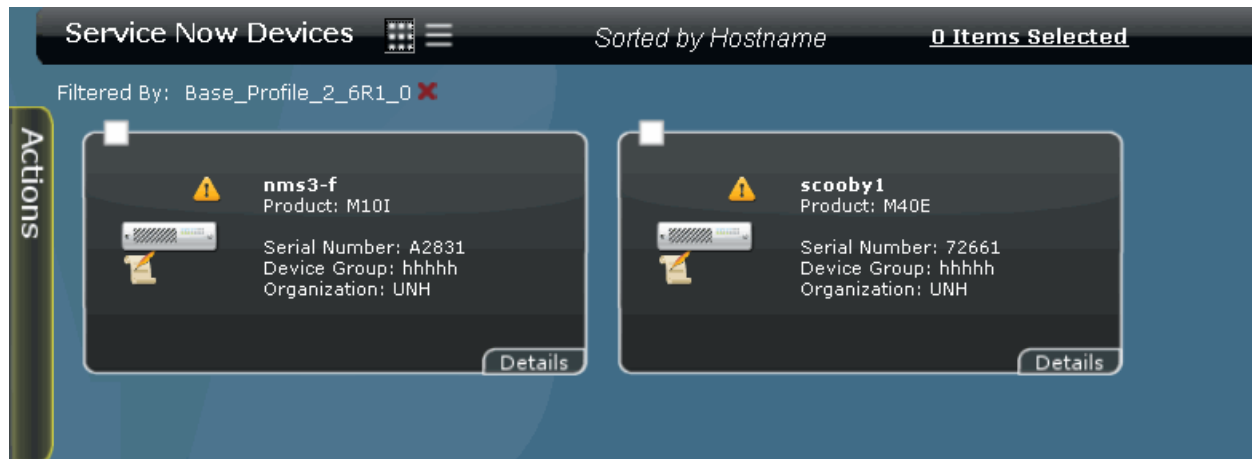
Using Service Now, you can view only those devices that are associated to a specific event profile. This task is disabled when you select an event profile that is not associated to any device.

To display devices associated to an event profile:

1. From the Service Now task ribbon, select **Administration > Event Profiles**.
The **View Event Profiles** page is displayed.
2. Select the event profile to view the devices associated with it.
3. Select **Show Associated Devices** from the **Actions** panel.

As shown in the following example, the **Manage Service Now Devices** page (Figure 18 on page 96) displays only the devices that are associated with the event profile (in the following example, **Base_Profile_2_6_R1_0**) that you selected.

Figure 18: Manage Service Now Devices page Displaying Device Associated to an Event Profile



- Related Documentation**
- Viewing an Event Profile on page 93
 - Pushing an Event Profile to Devices on page 94

Setting an Event Profile as Default

Service Now allows you to set an event profile as the default. When you select devices on which you want to install an event profile, the default event profile is automatically selected as the event profile that must be installed. The default event profile is represented by a unique icon on the **View Event Profiles** page. If you delete the default event profile, the latest event profile is automatically set as the default.

To set an event profile as the default:

1. From the Service Now task ribbon, select **Administration > Event Profiles**. The **Manage Event Profiles** page is displayed.
2. Select the event profile that you want to set as the default.
3. Use the **Actions** panel or right-click, and select **Set as Default**. The **Set As Default Profile** dialog box asks you for a confirmation.
4. Click **Confirm**.
The selected event profile is set as the default and is automatically selected as the event profile that must be installed when you select devices (**Manage Service Now Devices** page) on which you want to install an event profile. The default event profile (for example, Profile 2 in Figure 19 on page 97) is represented by a unique icon on the **View Event Profiles** page.

Figure 19: View Event Profiles page

View Event Profiles

Sorted by Created

0 Items Selected

Select: Page | None

Actions

<input type="checkbox"/>	Name	Description	AI Script Version	Created By	Created	Events Included	Events Excluded	Devices
<input type="checkbox"/>	test		2.5R1.0	super	Jan 26, 2011 7:05:48 PM IST	383	0	0
<input type="checkbox"/>	Base_Profile	Base Profile for Bundle Version: 2.6R1.0	2.6R1.0	Service Now	Jan 24, 2011 6:22:33 PM IST	376	0	2
<input type="checkbox"/>	New Profile	New Profile description	2.5R1.0	super		383	0	0
<input type="checkbox"/>	 Profile 2	Profile 2 description	2.5R1.0	super		20	363	1

- Related Documentation**
- Displaying Devices Associated with an Event Profile on page 95
 - Cloning an Event Profile on page 91
 - Pushing an Event Profile to Devices on page 94

Exporting Events Data in Excel Format

Service Now enables you to export events data into Excel file format and save it on your local file system.

To export events data into Excel file format:

1. From the Service Now task ribbon, select **Administration > Event Profiles**. The **Manage Event Profiles** page is displayed.
2. Double-click the event profile whose event activity you want to export into the Excel file format.
The **Event Profile Detail** dialog box displays details about the event activity that are associated to the event profile that you selected.
3. Click the **Export events to excel** link.
The **Opening ProfileEvents.xls** dialog box allows you to open or save the Excel file.
4. To open the Excel file, select **Open with**.
To save the Excel file on your local file system, select **Save File** and navigate to the folder where you want to save the excel file.
5. Click **OK**.
The information that is displayed in 5 tabs in the **Event Profile Detail** dialog box, is displayed in 5 separate worksheets in the Excel file.

- Related Documentation**
- Displaying Devices Associated with an Event Profile on page 95
 - Cloning an Event Profile on page 91
 - Pushing an Event Profile to Devices on page 94

Script Bundles Overview

script bundles, also known as AI-Script bundles, are specialized Juniper Networks operational and event scripts that detect events and provide information for analysis. To provide this information, AI-Scripts periodically collect intelligence information and package all incident and intelligence event data into a structured format called a Juniper Message Bundle (JMB). These JMBs are collected and displayed by Service Now. Script bundles are downloaded from the Juniper Networks software download Web site, and are installed on Service Now devices running JUNOS Release 9.0 or later.

- What AI-Scripts Do on page 98
- Events Detected by AI-Scripts on page 98
- JMB Contents on page 98
- Managing Script Bundles using Service Now on page 99

What AI-Scripts Do

AI-Scripts perform the following functions:

- React to specific incident events that occur on devices and provide relevant information about the problems for analysis.
- Periodically collect data on events that can be used to predict and prevent risks in the future.
- Package all incident and information event data into a structured format called a Juniper Message Bundle (JMB) and send it to Service Now. You can configure Service Now to send event data to Juniper Support Systems (JSS). JSS collects incident and device snapshots from Service Now and sends information messages back to Service Now specifically for your network.

AI-Scripts operate in a reactive (incident-driven) mode. When a trigger event occurs and is detected on a device, an AI-Script is executed. The AI-Script builds a Juniper Message Bundle (JMB) with event and router data, and sends it to Service Now. Each AI-Script corresponds to a specific device event. The list of device events that can be detected and reported evolves over time.

Events Detected by AI-Scripts

AI-Scripts detect the following types of events:

- Common software events, including daemon and Packet Forwarding Engine crashes
- Common hardware events, such as PIC alarms
- Hardware platform-specific events, such ASIC issues

JMB Contents

The JMB for incidents and informational JMBs contains the following:

- Manifest—basic router and event data
- Trend data—device counters, statistics, and settings

- Attachments—show command output for the incident event.

Managing Script Bundles using Service Now

After you upload script bundles to Service Now, to be able to install the script bundle on devices, you must associate the script bundle to an event profile (see “Event Profiles Overview” on page 87). An event profile is a set of event scripts that are selected from an AI-Script bundle. When you install an event profile on Juniper Networks devices, the event scripts selected from the script bundle are installed on the devices and these scripts provide the information needed to automatically detect and report problem (incident) and information events. Service Now uses Device Management Interface (DMI) to install and uninstall event profiles on devices. DMI is an extension to the NETCONF network management protocol.

The **Manage Script Bundles** page provides a central point for managing script bundles that have been downloaded from the Juniper Networks software download site. Service Now allows you to upload script bundles to Service Now, set a script bundle as the default, and delete script bundles. When you create an event profile, the default script bundle is automatically selected as the script bundle from which you select event scripts to associate with the event profile.

Related Documentation

- Adding a Script Bundle to Service Now on page 99
- Adding an Event Profile on page 89
- Setting a Script Bundle as Default on page 100
- Deleting a Script Bundle from Service Now on page 101

Adding a Script Bundle to Service Now

The **Manage Script Bundles** page provides a central point for managing script bundles (also known as AI-Script install packages) that have been downloaded from the Juniper Networks software download site. The script bundles must be located locally to the system running the Service Now application. You need Service Now administrator privileges to add a script bundle.

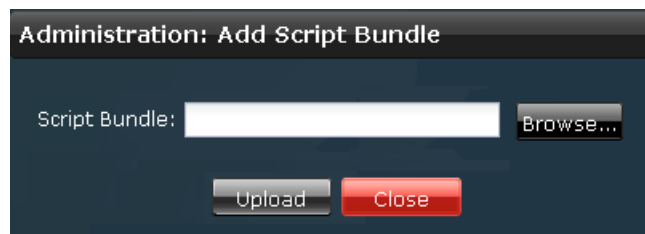
After you add a script bundle to Service Now, to be able to install the script bundle on devices you must first create an event profile using this script bundle. See “Adding an Event Profile” on page 89.

To add a script bundle:

1. From the Service Now task ribbon, select **Administration > Script Bundles > Add Script Bundle**.

The **Administration: Add Script Bundle** page is displayed as shown in Figure 20 on page 100.

Figure 20: Administration: Add Script Bundle Dialog Box



2. Click **Browse**.

The File Upload window is displayed.

3. Locate the script bundle and click **Upload**.

The selected script bundle is uploaded into Service Now and is displayed on the **Manage Script Bundles** page.

**Related
Documentation**

- Script Bundles Overview on page 98
- Setting a Script Bundle as Default on page 100

Setting a Script Bundle as Default

Service Now allows you to set a script bundle as the default. When you create an event profile, the default script bundle is automatically selected as the script bundle from which you select event scripts to associate with the event profile. The default script bundle is represented by a unique icon on the **Manage Script Bundles** page. If you delete the default script bundle, the latest script bundle to be uploaded is automatically set as the default.

To set a script bundle as the default:

1. From the Service Now task ribbon, select **Administration > Script Bundles**.
The **Manage Script Bundles** page lists the available script bundles.
2. Select the script bundle that you want to set as the default.
3. Right-click your selection, or use the **Actions** panel and select **Set as Default Bundle**.
The **Set as Default Bundle** dialog box prompts you to confirm.
4. Click **Confirm**.

The selected script bundle is set as the default and is represented by a unique icon on the **Manage Script Bundles** page.

**Related
Documentation**

- Script Bundles Overview on page 98
- Deleting a Script Bundle from Service Now on page 101

Deleting a Script Bundle from Service Now

With Service Now administrator privileges, you can delete script bundles.



NOTE: You cannot delete the preloaded script bundle that is available with Service Now.

To delete a script bundle:

1. From the Service Now task ribbon, select **Administration > Script Bundles**.

The **Manage Script Bundles** page lists the available script bundles.

2. Select the script bundle that you want to delete.
3. Select **Delete Script Bundles** from the Actions panel.

The **Delete AI-Scripts** dialog box prompts you to confirm the deletion.

4. Click **Delete**.

Service Now deletes the script bundle from the database and returns to the **Manage Script Bundles** page.

Related Documentation

- Script Bundles Overview on page 98
- Adding a Script Bundle to Service Now on page 99

CHAPTER 16

Global Settings

- Configuring Global Settings on page 103
- Adding an SNMP Server on page 106
- Editing and Deleting an SNMP Server on page 107
- Configuring Proxy Server Settings on page 108

Configuring Global Settings

You can use the Service Now global settings to perform the following tasks:

- Set the interval to scan devices for informational Juniper Message Bundles (JMBs).
- Set the SMTP server (IP address or hostname).
- Verify the connection status of Service Now to Juniper Support Systems (JSS) or Service Now to partner proxy (from end customer mode).
- Connect the end customer's Service Now application to the partner proxy.

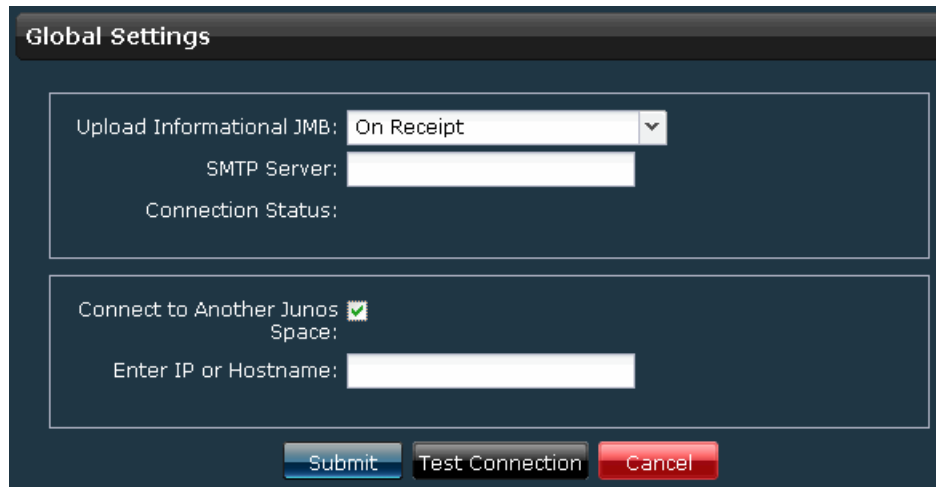
Using the Service Now **Global Settings** page, a Service Now end customer can also connect to a partner's Service Now application. When the Service Now application of an end customer connects to that of a partner, Junos Space uses a self-signed security certificate. Although Junos Space does not trust this method of identification, it automatically accepts the certificate to ensure that the communication between the partner and the end customer is encrypted. After you connect to the partner proxy's Service Now application, you enter end customer mode. You cannot revert to standard or partner proxy modes. After you connect to the partner proxy Service Now application, you can add an organization using the credentials provided by the partner. See "Adding an Organization" on page 65. After the connection of the organization is validated, you can submit incidents and iJMBs to, and open cases with, the Service Now partner.

For more information about standard, partner, and end customer modes, see "Service Now Modes" on page 9.

To configure Service Now global settings:

1. From the Service Now task ribbon, select **Administration > Global Settings**.

The **Global Settings** page is displayed.



2. Add your Service Now settings.

For a description of the fields on the **Global Settings** page, see Table 15 on page 105.



NOTE: The **Connect to Another Junos Space** check box is available only in Service Now end customer mode.

3. Click **Test Connection**.

The connection to JSS is tested and the result is displayed as **JSS Connection Status**.

4. Click **Submit**.

This action saves the Service Now settings that you specified and updates the Service Now service with these new settings.

Table 14 on page 104 describes the command buttons on the **Global Settings** page.

Table 14: Global Settings Command Buttons

Button Name	Description	Privileges	Enabled/Disabled	Results
Submit	Saves any modified Service Now global settings and updates the Service Now service with these new settings	Service Now Admin Settings	Enabled if you have administrator privileges	Saves settings that were modified.
Test Connection	<ul style="list-style-type: none"> In standard or partner proxy modes, verifies the organization's connectivity with JSS In end-customer mode verifies the organization's connectivity with the partner's Service Now application 	Service Now Admin Settings	Enabled if you have administrator privileges	Displays the Connection Status as Success or Failed.

Table 14: Global Settings Command Buttons (*continued*)

Button Name	Description	Privileges	Enabled/Disabled	Results
Cancel	Withdraws the submission of modified settings	Service Now Admin Settings	Not applicable	Navigates back to the Global Settings page without saving the entries.

Table 15 on page 105 describes the fields displayed in the tabular view of the **Global Settings** page.

Table 15: Global Settings Parameters

Name	Description	Privileges	Range/Length	Default
Upload Informational JMB	Interval when a newly detected Informational JMB is sent to JSS: <ul style="list-style-type: none"> On Receipt Daily Weekly 	Service Now administrator privileges	Not applicable	On Receipt
SMTP Server	Destination server that Service Now can use to send information You can enter either the IP address or the hostname. <ul style="list-style-type: none"> IP Address: IP address of the network management station where Service Now trap destinations are sent. Hostname: Identifier used for network communication between Service Now and a Junos OS device. For example, it can be a hostname (host-name.juniper.net). 	Service Now administrator privileges	255 characters	Blank
Connection Status	Status of connection from Service Now to JSS If Service Now is operating in end customer mode, the connection status between Service Now and the partner proxy is displayed.	Service Now Partner	<ul style="list-style-type: none"> Success — URL is responsive No route to host Connection refused The Home Base server is temporarily unable to service your request 	Blank
Connect to Another Junos Space	IP address or hostname of the Service Now partner proxy that can be used to send information to and receive information from the partner proxy. This field is not displayed when Service Now operates in standard mode and partner proxy mode.	Service Now End Customer	Not Applicable	Blank

- Related Documentation**
- Organizations Overview on page 63
 - Configuring Proxy Server Settings on page 108

Adding an SNMP Server

You can specify a destination for SNMP traps to be sent when a Service Now notification policy is triggered. SNMP traps are sent to these destinations only when the notification policy specifies this action. In **Service Now > Administration > Global Settings > SNMP Configuration**, the specified trap destinations are displayed.

To add and manage SNMP servers, you must have Service Now administration privileges.

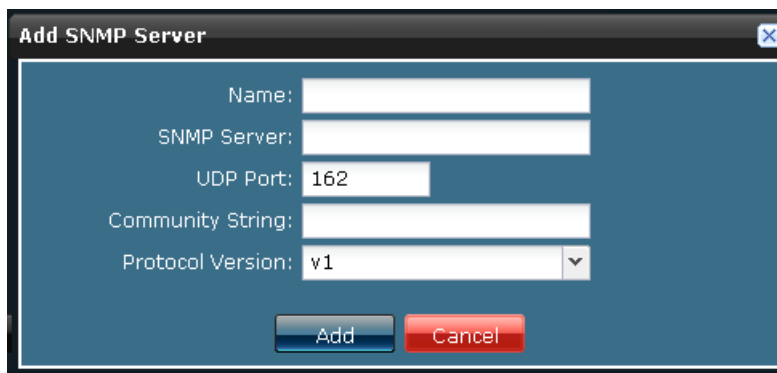
To add an SNMP server:

1. From the Service Now task ribbon, select **Administration > Global Settings > SNMP Configuration**.

The **SNMP Servers** page is displayed.

2. Click **Add**.

The **Add SNMP Server** dialog box is displayed.

The image shows a dialog box titled "Add SNMP Server" with a close button in the top right corner. The dialog box has a blue background and contains several input fields: "Name:" with a text box, "SNMP Server:" with a text box, "UDP Port:" with a text box containing "162", "Community String:" with a text box, and "Protocol Version:" with a dropdown menu showing "v1". At the bottom of the dialog box are two buttons: "Add" (blue) and "Cancel" (red).

3. Enter a name for the SNMP server, using alphanumeric values.
4. In the **SNMP Server** field, enter the SNMP server that is the IP address or hostname of the network management station where Service Now SNMP traps are sent. Do not use special characters.
5. Enter the UDP port number.

The User Datagram Protocol (UDP) port is a mechanism whereby a computer can simultaneously support multiple communication sessions with other computers and programs on the network. A port directs the request to a particular service that can be found at that IP address. The default UDP Port number is 162.
6. Enter a community string using only alphanumeric characters.

A community string is a password that allows access to a network device. It defines the community of people that can access the SNMP information on the device.

7. Select the protocol version from the list that specifies the SNMP versions.
8. Click **Add**.

The specified SNMP server is added to the Service Now database.

Loading MIBs

When using an MIB browser or other SNMP trap receivers such as HP OpenView to monitor the devices with SNMP, the following MIB files must be loaded. The **jnx-smi.mib** file must be loaded first:

1. jnx-smi.mib
2. jnx-ai-manager.mib

- Related Documentation**
- Configuring Global Settings on page 103
 - Configuring Proxy Server Settings on page 108

Editing and Deleting an SNMP Server

SNMP servers are the destination for SNMP traps to be sent when a Service Now notification policy is triggered. You can modify the parameters of these SNMP servers and also delete them.

Editing an SNMP Server

To edit an SNMP server:

1. From the Service Now task ribbon, select **Administration > Global Settings > SNMP Configuration**.

The **SNMP Servers** page is displayed.

2. Select the SNMP server whose parameters you want to modify.
3. Select **Edit** from the Actions panel.

The **Edit SNMP** dialog box is displayed.

4. Make the desired changes to the parameters.
5. Click **Save**.

The changes are saved in the Service Now database. To verify, you can view the changes on the **SNMP Servers** page.

Deleting an SNMP Server

To delete an SNMP server:

1. From the Service Now task ribbon, select **Administration > Global Settings > SNMP Configuration**.

The **SNMP Servers** page is displayed.

2. Select the SNMP server that you want to delete.

3. Select **Delete** from the Actions panel.

The selected SNMP server is deleted from the Service Now database and is no longer displayed on the **SNMP Servers** page.

**Related
Documentation**

- Configuring Global Settings on page 103
- Configuring Proxy Server Settings on page 108

Configuring Proxy Server Settings

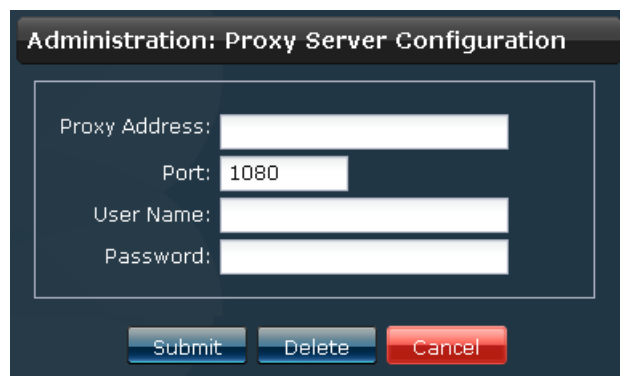
You can configure Service Now to work with a proxy server. When you connect to a proxy server, all communication to and from JSS happens through the proxy server. Both SOCKS and HTTP proxies are supported in Service Now.

The proxy server evaluates the request according to the filters specified. For example, it may filter traffic by IP address or protocol. When the request is validated, the proxy provides the resource by connecting to the relevant server and requesting the service on behalf of the client.

To configure the proxy server settings:

1. From the Service Now task ribbon, select **Administration > Global Settings > Proxy Server Configuration**.

The **Administration: Proxy Server Configuration** dialog box is displayed.

The image shows a dialog box titled "Administration: Proxy Server Configuration". It has a dark blue header bar with the title in white. The main area is white and contains four labeled text input fields: "Proxy Address:", "Port:", "User Name:", and "Password:". The "Port:" field has the value "1080" entered. At the bottom of the dialog, there are three buttons: "Submit" (blue), "Delete" (blue), and "Cancel" (red).

2. Enter the proxy address as a valid IP address or a valid hostname.
3. Specify the port on which the proxy server communicates with JSS.
The default port number is 1080.
4. Enter the login user name for authentication.
5. Enter the password that the identified user can use to log in.
6. Click **Submit**.

The proxy server settings are saved in the Service Now database.

- Related Documentation**
- [Configuring Global Settings on page 103](#)
 - [Adding an SNMP Server on page 106](#)

PART 5

Index

- Index on page 113

Index

A

adding devices.....	80
ai-script	
install.....	80
uninstall.....	84

C

conventions	
notice icons.....	xv
text.....	xv
customer support.....	xvi
contacting JTAC.....	xvi

D

dashboard overview	
Dashboard Gadgets.....	14
Service Now Workspaces.....	13
deleting	
device.....	85
device group.....	75
iJMB.....	46
incident.....	35
information message.....	43
notification policy.....	57
organization.....	69
device	
associate with device group.....	85
device group	
create.....	73
modify.....	74
documentation	
comments on.....	xvi

E

end customer mode.....	9
export device data	
CSV/excel.....	84
export iJMB	
html.....	45

G

global settings	
global.....	103
proxy server.....	108
snmp server	
add	106
edit/delete.....	107

I

Icons.....	17
incident	
assigning owner.....	32
export to HTML/excel.....	34
flagging.....	33
submitting.....	36
information message	
assign owner.....	42
flagging.....	42

J

JMB error.....	49
----------------	----

M

manuals	
comments on.....	xvi
modify submit case options.....	38

N

notice icons.....	xv
notification policy	
create.....	52
enable/disable.....	57

O

organization	
add.....	65
modify.....	68
run in test mode.....	71
test connection to JSS.....	70

overview	
administration.....	59
ai-scripts.....	98
device groups.....	73
device snapshots.....	45
devices.....	77
Incidents.....	31
messages.....	41
notifications.....	51
organization.....	63
Service Central	29
 P	
partner proxy mode.....	9
 S	
scan iJMB for ipact.....	43
script bundle	
add.....	99
delete.....	101
Service Now Overview.....	3
support, technical See technical support	
 T	
technical support	
contacting JTAC.....	xvi
text conventions defined.....	xv
 U	
user roles.....	23
 V	
view	
case in case manager.....	37
iJMB details.....	46
incident details	36